Ana Cláudia Correia Carapinha

003273

RELATÓRIO DE ESTÁGIO CURRICULAR

Visão sobre a proteção de dados em Portugal

Relatório elaborado com vista à obtenção
do grau de Mestre em Direito

Orientadora do Relatório de Estágio: Professora Doutora Maria Eduarda Gonçalves

Coordenadora do Estágio na CNPD: Professora Doutora Filipa Calvão

Julho 2014

Página propositadamente deixada em branco

Declaração de Compromisso de Antiplágio

Declaro por minha honra que, de acordo com o artigo 20º-A do Regulamento do Segundo Ciclo de Estudos, o trabalho que apresento é original e que todas as fontes utilizadas na sua elaboração estão corretamente identificadas. Tenho consciência de que a utilização de elementos alheios não identificados constitui uma grave falta ética e disciplinar.

Página propositadamente deixada em branco

Declaração de contagem de carateres

Declaro que o corpo do presente trabalho, no qual se incluem a introdução, desenvolvimento e conclusão e ainda os espaços e notas de rodapé, ocupa um total de 196.655 carateres.

O resumo em português ocupa um total de 2235 carateres, incluindo espaços.

O resumo em inglês ocupa um total de 1994 carateres, incluindo espaços.

Página propositadamente deixada em branco

Lista de abreviaturas

ACC Schengen – Autoridade de Controlo Comum Schengen

ACSS- Administração Central do Sistema de Saúde

ACT – Autoridade para as Condições de Trabalho

APDM – Associação Portuguesa de Marketing Direto

ASC – Autoridade Supervisora Comum

CC – Código Civil

CNPD – Comissão Nacional de Protecção de Dados

CNPDPI – Comissão Nacional de Protecção de Dados Pessoais Informatizados

CP – Código Penal

CPP – Código de Processo Penal

CRP – Constituição da República Portuguesa

CT – Código do Trabalho

EUA- Estados Unidos da América

ICC Europol – Instância Comum de Controlo da Europol

IDT – Instituto da Droga e da Toxicodependência

INEM – Instituto Nacional de Emergência Médica

LEC – Lei dos Ensaios Clínicos

LPD – Lei de Proteção de Dados

OCDE- Organização para a Cooperação e Desenvolvimento Económico

SIA – Sistema de Informação Aduaneira

SIEM – Sistema Integrado de Emergência Médica

SIS – Sistema de Informação Schengen

UE – União Europeia

Página propositadamente deixada em branco

Resumo

A proteção de dados pessoais apresenta-se como uma matéria indiscutivelmente complexa e transversal e disso nos dá conta o presente relatório, resultado do estágio curricular realizado na Comissão Nacional de Protecção de Dados. Sendo a Comissão a entidade competente para o controlo e fiscalização dos tratamentos de dados pessoais, o tema em torno do qual este relatório foi elaborado é o da proteção de dados pessoais, analisado de várias vertentes.

A proteção de dados pessoais é, desde há algum tempo, um tema que levanta muitas preocupações, por se encontrar intimamente ligado a direitos fundamentais dos cidadãos, constitucionalmente protegidos. Os direitos fundamentais inerentes a cada um de nós são uma decorrência do artigo 1º da Constituição da República Portuguesa, no sentido em que a dignidade da pessoa humana se afirma como o primeiro valor em torno do qual o ordenamento jurídico português terá de se alicerçar. Por outras palavras, constitui a dignidade da pessoa humana o valor mais alto no ordenamento jurídico português.

Foi com o desenvolvimento das sociedades ao ponto que hoje as conhecemos que se afirmou a relevância da proteção dos dados pessoais dos cidadãos. Nas atuais sociedades, em que é possível saber praticamente tudo sobre todos, em que a curiosidade alheia parece não se preocupar com as lesões que desencadeiam aos direitos dos cidadãos, em que as novas tecnologias fazem surgir pretextos para o tratamento desmedido de dados pessoais e onde os próprios titulares dos dados parecem não se incomodar que informações sobre si deem a volta ao mundo, é importante que os ordenamentos jurídicos valorizem a proteção dos dados pessoais e as implicações das suas utilizações indevidas, na medida em que estes são o

espelho da identidade de cada um de nós e podem ser utilizados contra os seus titulares, causando danos irreparáveis aos direitos fundamentais dos mesmos.

Entendendo-se por proteção de dados pessoais a possibilidade de cada cidadão decidir da utilização dos seus dados e a forma como podem ser utilizados, podemos afirmar que a sua proteção depende essencialmente de cada um de nós, enquanto titulares de dados pessoais. Portanto, a proteção dos nossos dados começa em nós próprios.

Abstract

The personal data protection is presented as an indisputably complex and transversal subject and gives an account of this report, a result of curricular internship at the Portuguese Commission for Data Protection. The Commission is the competent authority for the control and supervision of personal data processing. The subject around which this report was prepared is the protection of personal data, analyzed in several aspects.

The protection of personal data is, for some time, a topic that raises many concerns, because it is closely linked to fundamental rights constitutionally protected. Fundamental rights inherent in each of us are a result of Article 1 of the Constitution of the Portuguese Republic, in the sense that the dignity of the human person is affirmed as the first value around which the Portuguese legal system will have to be based. In other words, is the dignity of the human person the highest value in the Portuguese legal system.

Was the development of societies to the point that we know today that has led to the importance to the personal data of citizens. In modern societies, it is possible to know everything about everyone and the curiosity of others seems not to worry about the injuries that affect the rights of citizens. Where new technologies make excuses for the excessive processing of personal data and where subjects do not seem to bother about their personal data crossing the world, it is important that jurisdictions give value the protection of personal data and the implications of its misuse, in that as these are the mirror of identity each of us and can be used against their owners, causing irreparable damage to the their fundamental rights.

Being understood as protection of personal data the possibility of each citizen to decide the use of their data and how they can be used, we can say that its

protection depends essentially on each of us, as holders of personal data. Therefore, the protection of our data begins in ourselves.

1. Introdução

A elaboração do presente relatório de estágio decorre da realização de um estágio curricular na Comissão Nacional de Protecção de Dados entre 14 de outubro de 2013 e 28 de fevereiro de 2014. Este relatório consiste na última fase para a conclusão do Mestrado em Ciências Jurídicas Forenses que frequento na Faculdade de Direito da Universidade Nova de Lisboa, sendo, posteriormente, submetido a prova pública.

A Faculdade de Direito da Universidade Nova de Lisboa permite aos seus mestrandos que aquando da parte não letiva do Mestrado, optem entre elaborar uma tese de mestrado ou realizar um estágio curricular com a consequente realização do relatório de estágio. A minha opção foi a de realizar um estágio, uma vez que vislumbrei mais vantagens com a realização do mesmo do que com a elaboração de uma tese (não desfazendo da utilidade das teses), no sentido em que me permitiu ter um contacto numa vertente profissional com as matérias, o que contribuiu para alcançar uma perspetiva diferente das mesmas. Com a realização do estágio aliei o conhecimento teórico com o conhecimento prático, o que considero uma mais-valia, principalmente para a obtenção de um grau académico com relevância como é o de Mestre, pois permite adquirir uma especialização prática das matérias, embora os quatro meses e meio de estágio, apesar de produtivos, jamais seriam suficientes para conhecer todas as implicações dos temas relacionados com a proteção de dados, por ser uma matéria de enorme vastidão e que com tudo se relaciona.

A escolha pela realização do estágio na Comissão Nacional de Protecção de Dados deveu-se sobretudo à minha curiosidade em conhecer como as matérias são tratadas no âmbito da Comissão, assim como o funcionamento desta instituição de tanta importância no contexto nacional e também europeu. Mais do que motivações pessoais, que naturalmente têm de estar presentes no momento da escolha do

âmbito do estágio, não podemos descurar da importância associada ao âmbito de atuação da Comissão Nacional de Protecção de Dados. A proteção de dados pessoais é cada vez mais uma urgência se tomarmos em consideração que vivemos numa sociedade de informação, em que são constantes os ataques à privacidade dos cidadãos, quer pela usurpação de identidades, quer pela utilização desmedida de dados pessoais, não só por entidades que pretendem guardá-los e, por vezes, fazer não se sabe bem o que com os mesmos, mas também por culpa dos próprios titulares dos dados que expõem a sua vida de forma inconsciente, muitas vezes sem terem noção das consequências que podem advir de comportamentos sociais e que, à partida, não têm maldade alguma. Numa sociedade da informação e na era da informática e das telecomunicações, em que as tecnologias estão mais avançadas do que nunca, em que praticamente tudo é viável, falar de privacidade é possível e mais do que possível é necessário.

Esta é uma matéria que não poderá ser desprezada pelos Estados, nem pelos cidadãos que os constituem e é pela sua extrema importância que me quis dedicar a ela nesta fase tão importante na vida de um estudante.

Estruturei o relatório de estágio da forma que me pareceu mais lógica, tendo iniciado com uma breve caraterização da Comissão Nacional de Protecção de Dados, passando no ponto seguinte por abordar mais aprofundadamente o estágio em si (o seu faseamento, expetativas e relevância). Descrevo também as atividades que desenvolvi no decorrer do estágio, que se relacionaram com o conhecimento da prática seguida pela Comissão a várias situações de modo concreto, nomeadamente, através do contacto com processos cuja solução se encontra estipulada nas diversas Deliberações adotadas pela Comissão. Num último ponto, optei por analisar as atividades que desenvolvi durante o estágio, esclarecendo noções que foram referidas por diversas vezes e que entendi dever clarificar, até porque se reportam a conceitos elementares da proteção de dados e é fundamental para que o relatório seja dotado de alguma coerência. Neste último ponto, referi-me também a algumas questões que me foram diretamente colocadas por cidadãos, enquanto desempenhava as minhas funções no estágio e que achei pertinente trazê-las a análise neste relatório, sendo também um modo de fazer a minha própria análise de situações práticas.

2. Caraterização da Comissão Nacional de Protecção de Dados

2.1. A CNPD no âmbito nacional

É no Capítulo II da Lei n.º 10/91, de 29 de abril (Lei de Proteção de Dados Pessoais face à Informática)[1] que é determinada a criação de uma entidade com poderes de autoridade e controlo sobre o processamento de dados pessoais: a Comissão Nacional de Protecção de Dados Pessoais Informatizados (CNPDPI). A CNPDPI iniciou funções a 7 de janeiro de 1994.

Em 1998, com a aprovação da nova lei de proteção de dados pessoais – Lei n.º 67/98, de 26 de outubro[2] – as atribuições e competências da Comissão foram substancialmente alargadas, passando a designar-se apenas de Comissão Nacional de Protecção de Dados (CNPD). A constituição da CNPD fundamenta-se no n.º 2 do artigo 35º da Constituição da República Portuguesa.[3]

Nos termos do artigo 2º da Lei n.º 43/2004, de 18 de agosto (Lei de organização e funcionamento da CNPD)[4] e também do artigo 21º, n.º 1 da Lei n.º 67/98, de 26 de outubro, a CNPD afigura-se como uma entidade administrativa independente que funciona junto da Assembleia da República e tem como atribuição genérica controlar e fiscalizar o tratamento de dados pessoais, para que este se efetue no estrito respeito pelos direitos, liberdades e garantias consagrados na lei. Por ser uma entidade administrativa independente, não se encontra dependente de instruções ou recomendações do poder político para prosseguir o interesse público na proteção de uma área dotada de alguma sensibilidade.

Nos artigos 22º e 23º da Lei n.º 67/98, de 26 de outubro (Lei de Proteção de Dados, doravante designada LPD), encontramos um vasto conjunto de atribuições e competências da CNPD que expressam o papel decisivo no âmbito da utilização de

[1] Disponível em http://www.cnpd.pt/bin/legis/nacional/lei_1091.htm (consultado a 4 julho 2014).

[2] Disponível em http://www.cnpd.pt/bin/legis/nacional/LPD.pdf (consultado a 4 julho 2014).

[3] Artigo 35º (Utilização da informática) – n.º 2: "A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente".

[4] Disponível em http://www.cnpd.pt/bin/cnpd/Lei_43_2004.pdf (consultado a 4 julho 2014).

dados pessoais para diversas finalidades. A CNPD possui o poder para emitir pareceres sobre legislação ou instrumentos jurídicos em elaboração relativamente ao tratamento de dados pessoais, poderes de decisão no sentido de autorizar ou não um determinado tratamento de dados, de autorizar a transferência de dados pessoais, de fixar o prazo de conservação dos dados objeto de tratamento e também poder sancionatório, poderes de investigação e fiscalização, motivados quer por queixas apresentadas pelos cidadãos quer por iniciativa da Comissão, que poderão conduzir à aplicação de sanções por incumprimento das normas de proteção de dados pessoais. Inerentes ao poder de fiscalização estão os poderes de autoridade essenciais ao desempenho daquele.[5]

A CNPD assume também funções pedagógicas no cumprimento do disposto no artigo 23º, n.º 1, alínea p) da LPD. A alínea m) do referido preceito atribui à CNPD funções de representação internacional que, como perceberemos no ponto seguinte, são bastante amplas.

Em suma, a Comissão é a Autoridade Nacional de Controlo de Dados Pessoais.

2.2. A CNPD no âmbito internacional

O artigo 21º, n.º 4 da LPD, estabelece a cooperação da CNPD com autoridades de controlo de proteção de dados de outros Estados, o que nos remete para a atividade internacional da Comissão. A Comissão não só participa anualmente em vários encontros e conferências internacionais relativas à proteção de dados, como integra vários grupos de trabalho que em seguida desenvolverei de forma breve.

[5] No exercício dos poderes de fiscalização, a CNPD tem a faculdade de entrar em locais onde se encontrem os dados pessoais cujos tratamentos se pretende fiscalizar. Quem impedir a CNPD de exercer os seus poderes de fiscalização, poderá incorrer no crime de desobediência nos termos do artigo 348º do Código Penal. No entanto, a CNPD não poderá exercer esse poder em casas particulares, respeitando-se, assim, a inviolabilidade do domicílio.

2.2.1. Instância Comum de Controlo da Europol – ICC Europol[6]

A Convenção Europol cria um serviço Europeu de Polícia com o objetivo de estabelecer uma cooperação dos serviços policiais dos Estados-Membros com a finalidade de prevenção e combate do terrorismo, tráfico de estupefacientes e outras formas graves de criminalidade internacional.

A Instância Comum de Controlo da Europol foi instituída pelo artigo 24º da Convenção Europol [7] como uma entidade independente, competindo-lhe fiscalizar a atividade da Europol, quanto ao tratamento de dados pessoais, e garantir a legalidade do processamento e utilização de dados pessoais pela mesma.

Cabe à CNPD a representação do Estado Português na Instância Comum de Controlo da Europol, tal como dispõe o artigo 2º da Lei n.º 68/98, de 26 de outubro.

2.2.2. Autoridade de Controlo Comum Schengen – ACC Schengen

O Acordo de Schengen, datado de 1995 e a sua respetiva Convenção de Aplicação [8] pretendiam criar um espaço de livre circulação de pessoas, através da eliminação dos controlos nas fronteiras internas dos Estados signatários e a instauração de um controlo único na entrada em território Schengen. Portugal ratificou o Acordo e a Convenção em 1993, mas só em 1995 esta foi aplicada.

A Convenção estabelece um Sistema de Informação Schengen (SIS) nos artigos 92º a 101º e visa preservar a ordem e segurança públicas, bem como a aplicação das disposições da Convenção (artigo 93º), facilitando, assim, uma cooperação mais estreita entre as autoridades de fronteira, melhorando a cooperação

[6] Mais informações em http://europoljsb.consilium.europa.eu/about.aspx?lang=pt (consultado a 4 julho 2014).

[7] Disponível em http://www.dgpj.mj.pt/sections/leis-da-justica/pdf-internacional/convencoes-europeias/convencao-europol/downloadFile/file/Conv_Europol.pdf?nocache=1218040457.92 (consultado a 4 julho 2014).

[8] Disponível em http://www.gddc.pt/cooperacao/materia-penal/textos-mpenal/ue/schb-9.html (consultado a 4 julho 2014).

policial e judicial em matéria penal, bem como a política de vistos, de imigração e de livre circulação de pessoas.

A fim de garantir uma adequada proteção dos dados pessoais existentes no sistema de informação, a Convenção de Schengen prevê a existência de uma autoridade nacional de controlo, responsável pela fiscalização da parte nacional do SIS e pela verificação de que o tratamento de dados integrados no SIS não atenta contra os direitos dos seus titulares. Essa autoridade nacional é a CNPD (cf. artigo 7º da Lei n.º 2/94, de 19 de fevereiro) [9].

Cabem igualmente à CNPD funções de representação na Autoridade de Controlo Comum (ACC Schengen), constituída por dois representantes das autoridades de proteção de dados de cada Estado-Membro, que está encarregada do controlo da secção central do SIS. Tem ainda como competências assegurar que o SIS cumpre as disposições em matéria de proteção de dados referidas na Convenção Schengen, bem como analisar as dificuldades decorrentes da sua aplicação ou interpretação.

Foi desenvolvido um novo sistema – SIS II – cujo regulamento de funcionamento remonta a 2006 (Regulamento n.º 1897/2006, de 20 de dezembro). A substituição do sistema visa responder às novas questões relacionadas com o alargamento da União Europeia e colmatar algumas lacunas que a prática veio a demonstrar, constituindo uma *condição sine qua non* para a participação dos futuros Estados-Membros num espaço de segurança sem fronteiras internas.

2.2.3. Autoridade Supervisora Comum do Sistema de Informação Aduaneira

A Convenção que cria um Sistema de Informação Aduaneira tem por objetivo prestar assistência na prevenção, investigação e repressão de infrações graves à legislação nacional, aumentando, através da rápida divulgação de informações, a eficácia dos processos de cooperação e controlo das administrações aduaneiras dos Estados-Membros.

Para exercer o controlo em matéria de proteção de dados pessoais do Sistema de Informação Aduaneira (SIA), foi criada, em 2001, uma Autoridade Supervisora

[9] Disponível em http://www.cnpd.pt/bin/legis/nacional/Lei2-94-Schengen.pdf (consultado a 4 julho 2014).

Comum (ASC), constituída por representantes de cada Estado-Membro, na qual a CNPD participa.

A ASC fiscaliza o sistema de informações e examina as dificuldades de aplicação ou interpretação da Convenção, designadamente no que diz respeito ao direito de acesso dos cidadãos aos dados constantes do sistema.

2.2.4. Grupo de Trabalho das Telecomunicações

Foi criado em 1983, por iniciativa da autoridade de proteção de dados do estado de Berlim, onde tem a sua sede. Este grupo de trabalho reúne não só representantes das autoridades de proteção de dados, como também representantes de organizações internacionais e dos setores das telecomunicações e visa debater as implicações da utilização das novas tecnologias das telecomunicações na privacidade dos cidadãos.

A CNPD participa na atividade deste grupo de trabalho.

2.2.5. Grupo de Trabalho de Proteção de Dados

A Diretiva de Proteção de Dados – Diretiva n.º 95/46/CE, de 24 de outubro[10] - prevê no seu artigo 29º, a criação de um grupo de trabalho independente, com caráter consultivo, constituído pelas autoridades de proteção de dados dos Estados-Membros, por um representante das autoridades criadas para os organismos comunitários e por um representante da Comissão Europeia.

Este grupo de trabalho, também designado por Grupo de Trabalho do Artigo 29º tem como principais atribuições analisar as questões relativas à aplicação da Diretiva n.º 95/46/CE, contribuindo para a sua maior uniformização, dar parecer à Comissão Europeia sobre o nível de proteção na comunidade e nos países terceiros, aconselhá-la sobre medidas a tomar para proteção de direitos e liberdades das pessoas, dar parecer sobre códigos de conduta elaborados a nível comunitário, fazer

[10] Disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:PT:HTML (consultado a 4 julho 2014).

recomendações sobre quaisquer questões de proteção de dados pessoais. A CNPD integra o grupo de proteção de dados da União Europeia.

3. Estágio

3.1. Duração e faseamento

O estágio que realizei na Comissão Nacional de Proteção de Dados teve a duração de quatro meses e meio, tendo-se iniciado a 14 de outubro de 2013 e terminado a 28 de fevereiro de 2014.

Nas primeiras duas semanas de estágio, como primeiro contacto com a matéria relativa à proteção de dados pessoais, li as inúmeras Deliberações elaboradas pela Comissão e também opiniões elaboradas pelo Grupo de Trabalho do Artigo 29º, que abordarei mais pormenorizadamente no ponto 4. Terminadas as leituras iniciais foi altura de começar a tomar contacto com os primeiros processos. Tive a oportunidade de trabalhar com processos relativos às mais diversificadas matérias: prescrição eletrónica de medicamentos, gestão do processo clínico, cessão de créditos, medicina no trabalho, gestão de utentes, estudos clínicos, gravações de chamadas e videovigilância. A temática da videovigilância foi abordada de várias vertentes. Desde os processos de contraordenação por realização de tratamento de dados pessoais decorrentes da instalação e utilização de sistemas de videovigilância sem autorização da Comissão, até às substituições de processos que se encontravam em formato de papel para formato eletrónico, no âmbito das quais adquiri inúmeros conhecimentos, devido às diversas questões que o preenchimento dos formulários para autorização de videovigilância[11] foram suscitando.

Na fase final do estágio estive no Gabinete de Atendimento ao Público.

Pode-se, portanto, afirmar que o estágio que me foi proporcionado foi bastante rico no que se refere à diversidade de temáticas que abordei e me permitiu ficar com conhecimentos básicos sobre algumas das principais questões relativas à proteção de dados pessoais.

[11] Formulários disponíveis na página da CNPD - http://www.cnpd.pt/bin/legal/forms_video.htm (consultado a 4 julho 2014).

3.2.Expetativas anteriores à realização do estágio

Quando estabeleci contacto com a CNPD com o intuito de realizar um estágio curricular, eram escassos os meus conhecimentos sobre proteção de dados, uma vez que a primeira abordagem com algumas questões foi em Direito da Comunicação, disciplina lecionada no segundo semestre do primeiro ano do mestrado. No entanto, a abordagem superficial à proteção de dados foi suficiente para que despertasse muitas curiosidades e também um profundo desejo de conhecer melhor a temática.

Quando fui contactada dizendo que me iriam proporcionar o estágio, fiquei muito contente, não só por ser o meu primeiro contacto profissional com uma área relacionada com o Direito, mas também por durante os quatro meses e meio de duração do estágio, poder integrar uma instituição de extrema importância no nosso quotidiano, conhecendo as suas práticas enquanto guardiã nacional do direito dos cidadãos à proteção dos seus dados pessoais.

Deste modo, apesar de receosa por estar ciente da responsabilidade que iria assumir ao estagiar numa entidade tão relevante como a CNPD e também com a possibilidade de não conseguir acompanhar as matérias, o empolgamento sempre falou mais alto, uma vez que por muito mal que o estágio corresse iria terminá-lo sempre com uma perspetiva diferente da que tinha no dia em que o iniciei e com uma particular sensibilidade em relação às práticas do dia-a-dia que julgava inofensivas, nunca esquecendo que estaria perante temas muito complexos, cuja resposta não é fácil nem unânime também por envolver direitos fundamentais dos cidadãos.

3.3.Relevância atribuída ao estágio

Um adjetivo carateriza o meu percurso na CNPD: enriquecedor. Desde logo, porque fui bem recebida pela excelente equipa de profissionais que integra a Comissão, que sempre se demonstraram atenciosos e disponíveis para me auxiliar. Por outro lado, porque tomei conhecimento de questões que jamais imaginei que se

suscitassem e que são merecedoras de toda a atenção. Por último, porque posso afirmar que, após a minha curta estadia na CNPD, olharei para as matérias sobre proteção de dados com os olhos de quem sabe como se processam os esforços no sentido de proteger os cidadãos dos atentados contra a sua privacidade.

O facto de a Comissão me ter proporcionado um estágio tão diversificado e de ter sido apoiada por pessoas com um currículo extraordinário nesta área, contribuiu para que me ambientasse facilmente às matérias que me foram sendo dadas a conhecer e para que a minha vontade de aprofundar os conhecimentos sobre proteção de dados crescesse.

Por estarmos perante uma temática que, de qualquer forma, está relacionada com todas as áreas do Direito e que envolve direitos com uma dimensão constitucional, este estágio assume uma importância fulcral na minha formação.

É importante que cada vez mais pessoas estejam alerta para as matérias suscitadas pela proteção de dados, não só para melhor se prevenir atentados aos direitos dos cidadãos, como também para existirem mais especialistas que ajudem na resolução dos problemas que vão surgindo e que partilhem as suas ideias.

Neste sentido, encaro o meu percurso na CNPD como uma mais-valia, pelo facto de ter contactado com realidades que muitas pessoas nunca tiveram oportunidade de conhecer, pelo menos da perspetiva da entidade que controla e fiscaliza o processamento de dados pessoais em Portugal.

Página propositadamente deixada em branco

4. Descrição das atividades desenvolvidas

Neste ponto desenvolverei os temas com os quais contactei durante a realização do estágio. Tal como referi no ponto anterior, o meu estágio iniciou-se com a leitura de algumas Deliberações elaboradas pela CNPD[12], como forma de primeiro contacto com a proteção de dados pessoais, para que conseguisse apreender quais as questões mais suscitadas e os problemas e soluções que se impõem. Apesar de ter lido Deliberações muito interessantes, optei por me referir apenas àquelas que estiveram relacionadas com processos que posteriormente contactei, a fim de não dispersar o conteúdo pretendido com este relatório de estágio. De qualquer forma, destaco a Deliberação relativa ao voto eletrónico[13], a Deliberação respeitante aos tratamentos de dados relativos à comunicação interna de atos de gestão financeira irregular[14] e a Deliberação sobre o tratamento de dados biométricos como forma de controlo de acessos e assiduidade[15], devido ao seu especial interesse.

Assim, procederemos à análise individual de cada Deliberação, uma vez que as matérias comentadas são bastante distintas entre si, correspondendo as ideias que irão ser explanadas ao conteúdo essencial das mesmas.

Importa, contudo, antes de avançarmos, delimitarmos o conceito de dados pessoais, assim como o de tratamento de dados. Para tal, iremos auxiliar-nos de dois pareceres do Grupo de Trabalho do Artigo 29º.

---

[12]Deliberações disponíveis em http://www.cnpd.pt/bin/orientacoes/orientacoes.htm (consultado a 4 julho 2014).

[13] Disponível em http://www.cnpd.pt/bin/orientacoes/Delib_voto_electronico.pdf (consultado a 4 julho2014).

[14] Disponível em http://www.cnpd.pt/bin/orientacoes/DEL765-2009_LINHAS_ETICA.pdf (consultado a 4 julho 2014).

[15] Disponível em http://www.cnpd.pt/bin/orientacoes/PRINCIPIOS-BIOM-assiduidade-acesso.pdf (consultado a 4 julho 2014).

4.1. Conceito de dados pessoais segundo a opinião 4/2007, de 20 de junho, do Grupo de Trabalho do Artigo 29º[16]

O Grupo de Trabalho do Artigo 29º[17] pretende com este parecer gerar um entendimento comum no espaço europeu sobre o conceito de dados pessoais, criando um guia que uniformize a aplicação das normas nacionais de proteção de dados pessoais, estipulando as situações em que estas terão aplicação.

A Diretiva n.º 95/46/CE, de 24 de outubro de 1995[18], relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, consagra uma noção ampla de dados pessoais na alínea a) do seu artigo 2º, pelo facto de consistir em qualquer informação que respeite a uma pessoa singular. Embora consagre uma noção ampla de dados pessoais, não significa que toda e qualquer situação se submeta ao âmbito de aplicação da Diretiva. As normas relativas à proteção de dados não se podem aplicar a situações a que o legislador não as pretendeu aplicar, sendo que os considerandos 26 e 27 da Diretiva[19] refletem o modo como aquele pretendeu que as normas fossem interpretadas e aplicadas.

O âmbito das normas de proteção de dados não pode ser ampliado de forma injustificada, tal como é de evitar a restrição indevida do conceito de dado pessoal. Deste modo, uma constatação se impõe. Para que as normas da Diretiva sejam aplicadas de forma adequada, primeiro há que certificar que o caso em concreto se

---

16 Disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf (consultado a 4 julho 2014).

17 O Grupo de Trabalho do Artigo 29º foi instituído pelo artigo 29º da Diretiva 95/46/CE e assume-se como um órgão europeu de caráter consultivo no que se refere à proteção de dados pessoais e à privacidade. Questão analisada no ponto 2.2.5. (Grupo de Trabalho de Proteção de Dados).

18 Disponível em http://www.cnpd.pt/bin/legis/internacional/95-46-CE.pdf (consultado a 4 julho 2014).

19 Segundo o Considerando 26 da Diretiva, os princípios de proteção de dados devem aplicar-se a qualquer informação que seja relativa a uma pessoa identificada ou identificável, sendo que a identificabilidade de um indivíduo determina-se tendo em conta os instrumentos que podem ser utilizados para o identificar. Os princípios de proteção de dados não se aplicarão aos dados que tenham sido tornados anónimos de forma irreversível, isto é, quando a pessoa já não seja identificável de forma alguma.
O Considerando 27 refere que a proteção dos titulares dos dados, deve estar presente quer o tratamento dos dados seja automatizado ou não, acrescentando que se o âmbito de proteção das normas dependesse das técnicas utilizadas nos tratamentos de dados, a proteção dos dados estaria condicionada.

insere no âmbito de aplicação da mesma, nos termos do artigo 3º e, em caso afirmativo, se as suas normas asseguram uma resposta jurídica adequada à proteção dos direitos individuais.

Aos dados que não se possam incluir na definição de dados pessoais consagrada na Diretiva, como é o caso de informações que não se relacionem com uma pessoa ou quando a pessoa não seja identificada ou identificável, não se aplicará a Diretiva[20], o que não significa que a lei nacional não se poderá aplicar. Os Estados-Membros podem estender o âmbito de aplicação da sua legislação que concretize disposições da Diretiva a situações não abrangidas pela sua legislação. De outra forma, existem outras normas que poderão demonstrar-se aptas a proteger determinada situação quando as normas de proteção de dados não se apliquem.

A definição de dados pessoais que consta do artigo 2º, alínea a) da Diretiva[21] abrange quatro elementos que se impõem analisar de forma mais precisa.

4.1.1. "Qualquer informação"

É este o elemento que atribui à noção de dados pessoais um conteúdo amplo. Para que a informação adquira a natureza de dado pessoal, não tem necessariamente de ser verdadeira. Do ponto de vista do conteúdo da informação, o conceito de dado pessoal inclui tanto informação considerada como dados sensíveis (como os descritos no artigo 8º n.º 1), como informação relativa a qualquer atividade realizada pela pessoa em questão. Já em relação ao formato que suporta a informação, o conceito de dado pessoal inclui informação contida em qualquer formato, podendo tratar-se de informação contida num papel ou num computador, ou informação

[20] Artigo 3º, n.º 2 da Diretiva

[21]

Artigo 2º
Definições

"Para efeitos da presente diretiva, entende-se por:

a) «Dados pessoais», qualquer informação relativa a uma pessoa singular identificada ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social".

contida numa mensagem de correio eletrónico ou em imagens de câmaras de videovigilância.

4.1.2. "Relativa a"

De forma geral, a informação considera-se relativa a uma pessoa individual quando se tratam de assuntos que estejam relacionados com essa pessoa e, grande parte das vezes, a relação da informação com o sujeito consegue estabelecer-se de forma simples existindo, porém, situações em que nem sempre assim é.

Entende o Grupo de Trabalho do Artigo 29º que quando a informação se refere à individualidade de uma pessoa, estamos perante dados referentes à sua identidade, às suas caraterísticas físicas ou à sua personalidade.

São três os elementos a ter em consideração para discernir se a informação se refere a uma pessoa singular: conteúdo, finalidade e resultado. Estes três elementos assumem-se como alternativos. Relativamente ao conteúdo, a informação tem de se referir a uma pessoa em particular. No elemento finalidade, a informação será utilizada pretendendo influenciar o estatuto ou o comportamento de uma pessoa. Já quanto ao elemento resultado, este verifica-se quando a informação tiver impacto nos direitos e interesses de uma determinada pessoa, ou seja, como resultado do tratamento da informação, a pessoa em causa terá de ser tratada de forma diferente comparativamente com outras pessoas.

4.1.3. "Pessoa singular"

As normas da Diretiva visam proteger pessoas singulares.[22] Segundo o artigo 6º da Declaração Universal dos Direitos do Homem[23], todos os indivíduos têm direito a ver reconhecida a sua personalidade jurídica (cf. artigo 6º), caracterizando-se esta como a capacidade para se ser sujeito de relações jurídicas[24], que se concretiza com o nascimento completo e com vida e cessa com a morte. Deste

[22] Considerando 2 da Diretiva.

[23] Disponível em http://afilosofia.no.sapo.pt/cidadania1.htm (consultado a 4 julho 2014).

[24] Artigos 66º e 67º do Código Civil.

modo, em princípio, os dados pessoais referem-se a pessoas vivas, não se considerando como tal dados de pessoas falecidas, pois estas não se consideram pessoas singulares nos termos da lei civil.

Os responsáveis por tratamentos de dados não conseguem determinar se aqueles dados pessoais em concreto se referem a uma pessoa viva ou não, logo, irão tratar os dados das pessoas já falecidas do mesmo modo que tratam os dados das pessoas vivas. Além disso, os dados relativos a pessoas falecidas podem estar relacionados com pessoas vivas e, assim sendo, poderão ser alvo das normas de proteção de dados.

Por outro lado, os dados pessoais de pessoas falecidas encontram-se protegidos pelo dever de confidencialidade dos médicos que não cessa com a morte dos pacientes. O mesmo sucede com o direito à imagem (cf. artigo 79º do Código Civil).

Se a proteção de dados pessoais se coloca quanto a pessoas falecidas, também se colocará em relação aos nascituros e a resposta dependerá do sistema legal próprio de cada Estado-Membro sobre o conceito de nascituro e suas implicações. Para concluir se a legislação protetora de dados pessoais de cada Estado se aplica a nascituros, tem de se considerar o sistema jurídico em particular[25].

O conceito de dados pessoais refere-se a pessoas singulares, o que leva a questionar se as pessoas coletivas são igualmente abrangidas por esse conceito encontrando-se também protegidas pelas normas de proteção de dados. Em determinados contextos, as referidas normas podem aplicar-se também às pessoas coletivas, na medida em que algumas informações referentes à pessoa coletiva são indissociáveis da pessoa singular, como é o caso do nome da empresa ser o nome da pessoa singular que a detém ou o caso do correio eletrónico da empresa utilizado por um trabalhador. Nestes casos, as informações referentes à pessoa coletiva são

[25] O nascituro é o ser humano ou um projeto de conceção de um ser humano, cujo nascimento é provável ou possível. Este conceito implica a distinção entre nascituro conceturo e nascituro concebido, correspondendo o primeiro ao projeto de conceção de um ser humano, cuja conceção e nascimento se preveem como possíveis, enquanto o segundo corresponde ao feto que se encontra em fase de gestação, ou seja, é um ser já concebido mas ainda não nascido. O Código Civil português estabelece no artigo 66º, n.º 2 que o reconhecimento dos direitos do nascituro depende do seu efetivo nascimento, o que significa que, apesar de não terem personalidade jurídica, a lei lhes reconhece direitos que se encontram dependentes do seu nascimento completo e com vida. Existe, contudo, tutela jurídica aos nascituros concebidos, no que se refere à esfera patrimonial (doações, heranças) e também às lesões que venham a sofrer durante a gestação que decorram de atos que originem problemas ou deformações.

inerentes à pessoa singular e, deste modo, consideram-se dados pessoais de uma pessoa singular, aplicando-se as normas de proteção de dados pessoais. [26]

4.1.4. " Identificada ou identificável"

Uma pessoa considera-se identificada quando, inserida num grupo de pessoas, se distingue dos outros membros do grupo. Por sua vez, a pessoa considera-se identificável quando é possível identificá-la. Uma pessoa pode ser diretamente identificável pelo nome, por ser o elemento identificador mais comum, todavia, o nome, só por si, pode não tornar a pessoa diretamente identificável sem, por exemplo, se recorrer a uma fotografia sua ou à sua data de nascimento, nos casos em que existam pessoas com o mesmo nome que possam confundir-se entre si. Por outro lado, a pessoa pode ser indiretamente identificável, por exemplo, por um número de telefone ou pela combinação de informações.

Segundo o Considerando 26 da Diretiva " (…) para determinar se uma pessoa é identificável, importa considerar o conjunto dos meios suscetíveis de serem razoavelmente utilizados (…)", ou seja, a possibilidade de individualizar uma pessoa, só por si, não torna a pessoa identificável. Quando o tratamento de dados pessoais não tem como finalidade desvendar a identidade do titular dos dados, as medidas que têm de ser adotadas a fim de inviabilizar a possibilidade de o identificar, assumem um papel muito importante, afigurando-se como uma condição para que a informação não se traduza em dados pessoais. Nos casos em que a finalidade do tratamento acarreta a identificação do titular dos dados, então o responsável pelo tratamento terá os meios adequados para identificar a pessoa em causa.

[26] Tal como a Diretiva de proteção de dados, a Lei de Proteção de Dados portuguesa pretende assegurar a legitimidade do tratamento de dados apenas de pessoas singulares, excluindo-se o tratamento de dados de pessoas coletivas, devido à incompatibilidade da natureza das mesmas com alguns direitos que se pretendem assegurar, pertence exclusivo das pessoas singulares. Porém, as pessoas coletivas podem estar abrangidas pelo âmbito de proteção de normas que sejam compatíveis com a sua natureza coletiva (artigo 12º, n.º 2 CRP), como é o caso do direito à inviolabilidade do domicílio e da sua correspondência.
O Parecer n.º 18/2000, de 5 de maio, publicado no Relatório da CNPD do ano 2000 (disponível em http://www.cnpd.pt/bin/decisoes/2000/htm/par/par018-00.htm) refere que "É cada vez mais duvidoso que possa continuar a considerar-se como exclusivo destinatário das medidas de proteção em matéria de dados pessoais as pessoas singulares, esquecendo as pessoas coletivas", acrescentando que "(…) o consenso quanto ao gozo de direitos pelas pessoas coletivas, desde que compatíveis com a sua natureza, e a larga convergência quanto à importância de salvaguardar as pessoas coletivas de intromissões lesivas da sua esfera pessoal, aconselha a que se reflita sobre uma possível ponderação da proteção das pessoas coletivas, em determinadas condições, nos tratamentos relativos aos seus dados pessoais".

Neste ponto, teremos de distinguir três tipos de dados: dados sob pseudónimo, dados codificados e dados anónimos.

A. Dados sob pseudónimo

O pseudónimo traduz-se num processo de disfarçar a identidade, com o objetivo de recolher dados relativos a uma pessoa, não se revelando a sua identidade. Os pseudónimos devem ser aleatórios e imprevisíveis e em número tão vasto que o mesmo pseudónimo não deverá ser utilizado mais do que uma vez. A eficácia da utilização de dados sob pseudónimo depende muito da possibilidade de serem revertidos e interligados a determinada pessoa.

A utilização de dados sob pseudónimo considera-se informação de pessoas indiretamente identificáveis, uma vez que existe a possibilidade do indivíduo ser identificado, devendo esse risco ser reduzido.

B. Dados codificados

Os dados codificados são informação relativa a indivíduos que se encontram individualizados por um código. Os dados codificados traduzem-se em informação relativa a pessoas identificáveis e, por isso, devem respeitar a legislação sobre proteção de dados. Este tipo de dados é vulgarmente utilizado em ensaios clínicos.

C. Dados anónimos

O conceito de dados anónimos consiste em informação referente a uma pessoa singular, na qual esta não possa ser identificada por qualquer pessoa. Os dados que foram tornados anónimos são dados que, anteriormente, se referiam a uma pessoa identificável, mas essa identificação não é mais possível. Nesse caso os princípios de proteção de dados não se aplicam.[27]

[27] Considerando 26 da Diretiva.

4.2. Princípio da limitação da finalidade segundo a opinião 3/2013, de 2 de abril, do Grupo de Trabalho do Artigo 29º[28]

Um dos princípios fundamentais da proteção de dados diz respeito à finalidade do tratamento de dados pessoais.[29] São duas as vertentes inerentes ao conceito da limitação da finalidade. Desde logo, os dados pessoais podem ser utilizados para uma finalidade específica, explícita e legítima, sendo esta a vertente da especificação da finalidade. Por outro lado, os dados pessoais não podem ser tratados de forma incompatível com a finalidade, sendo esta a vertente do uso compatível. Estas vertentes encontram-se consagradas no artigo 6º, n.º 1, alínea b) da Diretiva n.º 95/46/CE, de 24 de outubro.[30]

A especificação da finalidade é o primeiro elemento essencial para que se possa verificar a aplicação da legislação protetora de dados pessoais e para se averiguar a aplicabilidade dos restantes princípios. É também uma condição para avaliar a necessidade da interferência na vida privada dos titulares dos dados e contribuem para a transparência e para a certeza jurídica, o que garante a previsibilidade do tratamento de dados pessoais. A finalidade específica permite a implementação de quaisquer salvaguardas necessárias à proteção dos dados e eliminar o âmbito do processo de tratamento dos mesmos. Por sua vez, a proibição do uso incompatível assume-se como uma limitação ao uso adicional dos dados[31].

---

[28] Disponível em http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (consultado a 4 julho 2014).

[29] Nos termos do artigo 2º, alínea b) da Diretiva, entende-se por tratamento de dados pessoais" (…) qualquer operação ou conjunto de operações efetuadas sobre dados pessoais, com ou sem meios automatizados (…)". A mesma definição consta da Lei de Proteção de Dados portuguesa, no artigo 3º, alínea b).

[30] Artigo 6º, n.º 1,
Alínea b): "Recolhidos para finalidades determinadas, explícitas e legítimas, e que não serão posteriormente tratados de forma incompatível com essas finalidades".

[31] Última parte do considerando 28 da diretiva: " (…) que as finalidades dos tratamentos posteriores à recolha não podem ser incompatíveis com as finalidades especificadas inicialmente".

Segundo o Grupo de Trabalho, o tratamento dos dados para uma finalidade diferente daquela para que foram recolhidos, não significa necessariamente que o tratamento é absolutamente incompatível com a finalidade, uma vez que esta exige uma apreciação casuística, nomeadamente, através da análise da finalidade inicialmente prosseguida e da finalidade adicional, das expetativas dos titulares dos dados quanto à sua utilização, assim como da natureza dos dados pessoais e o impacto do seu tratamento nos titulares dos dados.

Proceder ao tratamento de dados pessoais de forma incompatível com a finalidade para que foram recolhidos, como dissemos acima, é proibido, sendo que o princípio da limitação da finalidade apenas pode ser restringido nas condições consagradas no artigo 13º da Diretiva n.º 95/46/CE. Não só o tratamento dos dados tem de ter o objetivo de salvaguardar interesses públicos específicos como é o caso da segurança pública, prevenção da criminalidade, entre outros, como tem de ser suficientemente preciso e afigurar-se necessário e proporcional. Face ao exposto, podemos então concluir que a Diretiva permite aos Estados-Membros que restrinjam o princípio da limitação da finalidade, desde que essa restrição se afigure necessária à salvaguarda de outros interesses. Foi elaborado um estudo intitulado "Avaliação da implementação da Diretiva de proteção de dados" que salientou que as disposições consagradas na Diretiva não se revelam eficazes na aplicação do princípio da limitação da finalidade, o que, aliado à flexibilidade da sua aplicação pelos Estados-Membros, originou interpretações e aplicações divergentes.

O Grupo de Trabalho alerta para a necessidade de existir uma interpretação harmoniosa deste princípio nos Estados-Membros, uma vez que um entendimento distinto pode levar a abordagens diferentes, o que é de evitar, pois uma abordagem incoerente pode enfraquecer a posição dos titulares dos dados.

4.3. Privacidade no local de trabalho

4.3.1. Tratamentos de dados no âmbito da gestão da informação dos serviços de segurança e saúde no trabalho[32]

A legitimidade para o tratamento de dados no âmbito da medicina no trabalho resulta do disposto nos artigos 281º a 284º do Código do Trabalho e da Lei n.º 102/2009, de 10 de setembro[33], que estabelece o regime jurídico da promoção da segurança e saúde no trabalho. Estes tratamentos afiguram-se legítimos na medida em que os serviços de segurança e saúde no trabalho decorrem de uma obrigação legal e, como tal, vão ao encontro do estipulado no artigo 7º, n.º2 da Lei de Proteção de Dados. Por outras palavras, por resultar de consagração legal, o tratamento destas categorias de dados pessoais é permitido quando, por motivos de interesse público importante, se assumir indispensável ao cumprimento de obrigações legais. Importa não esquecer que esta permissão de tratamento existe apenas quando o responsável pelo mesmo adotar as medidas de segurança previstas no artigo 15º da LPD e se assegurar garantias de não discriminação aos titulares dos dados, devendo ter em consideração não só as metodologias de recolha e processamento dos dados, mas também o modo como a informação circula, uma vez que, nos termos do artigo 7º da LPD, estamos perante um tratamento de dados pessoais sensíveis.

No âmbito dos serviços de segurança e saúde no trabalho, é necessária a recolha e tratamento de dados como os de identificação e de saúde, dados relativos à atividade profissional e dados sobre risco de doença profissional e doenças profissionais. Nestas categorias de dados pessoais, não se incluem os hábitos pessoais que, por regra, não podem ser objeto de tratamento pelo facto de o registo pormenorizado do consumo de álcool ou de estupefacientes se assumir uma devassa

[32] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/DEL_840_2010_MED_trabalho_actualizada.pdf (consultado a 4 julho 2014).

[33] Disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1158&tabela=leis&so_miolo (consultado a 4 julho 2014).

injustificada, excessiva e, por isso, potencialmente discriminatória, nos hábitos do trabalhador. Existe, contudo, exceção à regra, ou seja, na medida em que informações como o consumo de tabaco, drogas ou alcoolemia se possam relacionar com determinados sintomas e patologias ou com outros dados de saúde, admite-se a recolha e tratamento de informações desta natureza no âmbito da finalidade prosseguida pelos serviços de segurança e saúde no trabalho. O mesmo sucede com os dados relacionados com a vida sexual, pois apenas se admite o seu registo nas situações em que se possam relacionar com patologias específicas ou com outros dados de saúde.

Já no que se refere aos dados nacionalidade, raça e origem étnica, o seu tratamento não se afigura pertinente para a finalidade de medicina no trabalho, pelo elevado risco de discriminação que acarreta. De certa forma, este tratamento é proibido também por algumas disposições que visam evitar qualquer modo de discriminação em função da raça, cor, nacionalidade ou origem étnica, como é o caso dos artigos 23º a 28º do Código do Trabalho, da Lei n.º 7/82, de 29 de abril, que aprova a adesão à Convenção Internacional sobre Eliminação de Todas as Formas de Discriminação Racial, adotada pela Assembleia Geral das Nações Unidas em 21 de Dezembro de 1965[34] e também da Lei n.º 134/99, de 28 de agosto,[35] que proíbe as discriminações no exercício de direitos por motivos baseados na raça, cor, nacionalidade ou origem étnica.

A responsabilidade dos tratamentos de dados no âmbito da gestão da informação dos serviços de segurança e saúde no trabalho cabe exclusivamente ao empregador. A informação de saúde jamais pode ser comunicada aquele, devendo ser de acesso exclusivo ao médico do trabalho ou a outros profissionais de saúde obrigados a sigilo profissional, sob a direção e controlo deste. As observações clínicas relativas à informação de saúde são anotadas em lugar próprio, dando origem ao preenchimento de uma "ficha de aptidão", que não pode conter elementos sujeitos a segredo profissional (artigo 110º, n.º 3 da Lei n.º 102/2009, de

[34] Disponível em http://bo.io.gov.mo/bo/i/98/37/leiar07.asp (consultado a 4 julho 2014).

[35] Disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=230&tabela=leis (consultado a 4 julho 2014).

10 de Setembro) e que será entregue ao empregador, para que este seja informado dos resultados necessários para a sua tomada de decisão em matéria de emprego.

Existindo circulação da informação de saúde em rede, essa transmissão de dados deve ser cifrada.

4.3.2. Tratamentos de dados com a finalidade de medicina preventiva e curativa no âmbito dos controlos de substâncias psicoativas efetuados a trabalhadores[36]

Os tratamentos de dados efetuados no âmbito de controlo de substâncias psicoativas, por permitirem a identificação de perfis de comportamento dos trabalhadores que sejam alvo deste tipo de controlo, assumem-se como tratamentos de dados sensíveis na aceção do artigo 7º da LPD, não só por estarmos perante dados de saúde dos trabalhadores, mas também por estarem relacionados com a vida privada dos mesmos, pelo que, nos termos do artigo 28º, alínea a) da LPD, estão sujeitos a controlo prévio, o que significa que estes tratamentos de dados não se podem iniciar sem a autorização da CNPD.

Tal como resulta da Deliberação elaborada pela CNPD, podemos dispor por categorias os dados que podem ser objeto de tratamento, tendo em conta a finalidade específica que é prosseguida.[37] Desde logo, podem ser tratados dados de identificação do trabalhador, dados de saúde que se relacionem com o consumo de substâncias psicoativas, as próprias substâncias detetadas, as circunstâncias em que os testes serão aplicados, dados de identificação dos profissionais de saúde envolvidos, a frequência do controlo e as datas em que se realiza, bem como o seu resultado e os procedimentos adotados caso o resultado seja positivo.

Quando estas informações se afigurem necessárias para avaliar a aptidão dos trabalhadores, subsumem-se ao conceito de informação médica prevista no artigo 5º da Lei n.º 12/2005, de 26 de janeiro)[38]. Na informação de saúde incluem-se os

[36] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/20_890_2010.pdf (consultado a 4 julho 2014).

[37] Página 25 da Deliberação.

[38] Disponível em http://www.cnpd.pt/bin/legis/nacional/Lei12-2005.pdf (consultado a 4 julho 2014).

resultados dos testes efetuados ao trabalhador que, em caso algum, poderão ser comunicados ao empregador, que apenas deverá saber do estado de aptidão ou não aptidão do trabalhador para exercer as funções que lhe competem.

No que se refere à legitimidade para os tratamentos descritos, esta decorre do interesse público importante subjacente ao tratamento - perigo do consumo das substâncias para o próprio trabalhador ou para terceiros - condição de legitimidade prevista no artigo 7º, n.º2 da LPD e também no artigo 19º, n.º 1 do Código do Trabalho a ser atendida pela responsável pelo tratamento, a entidade empregadora.

Do protocolo "Prevenção de Riscos em Meio Laboral" desenvolvido entre o Instituto da Droga e da Toxicodependência (IDT) e a Autoridade para as Condições de Trabalho (ACT), resultou um documento intitulado de "Segurança e Saúde no Trabalho e a Prevenção do Consumo de Substâncias Psicoativas: linhas orientadoras para a intervenção em meio laboral"[39] que, como a designação indica, estabeleceu os princípios orientadores de intervenção em meio laboral, no que se refere ao consumo de substâncias psicoativas pelos trabalhadores. Deste documento ressaltam ideias relevantes a serem consideradas. A livre adesão do trabalhador é uma condição fulcral da eficácia da intervenção em meio laboral, uma vez que o tratamento e reabilitação do trabalhador só pode resultar se este aceitar submeter-se a tal processo, além de que os trabalhadores que aceitem submeter-se a intervenção clínica não podem ser discriminados pelo empregador, devendo este garantir o posto de trabalho daqueles e todos os direitos que lhes assistem.

A CNPD entende que não existindo razões para efetuar o controlo destas substâncias num trabalhador, esse controlo não é aceitável do ponto de vista dos princípios da proporcionalidade, adequabilidade e razoabilidade. [40] Isto significa que não existindo condições de legitimidade para o tratamento de dados analisado, este não é legalmente permitido, pelo facto de não se afigurar adequado sujeitar a generalidade dos trabalhadores à realização de testes de alcoolemia, sendo imposição do princípio da igualdade que situações distintas sejam tratadas de forma diferente.

[39] Disponível em http://www.act.gov.pt/%28pt-PT%29/crc/PublicacoesElectronicas/Documents/LinhasOrientadorasParaIntervencaoEmMeioLaboral_2011_23.pdf (consultado a 4 julho 2014).

[40] Página 21, 2º parágrafo da Deliberação.

4.3.3. Tratamentos de dados decorrentes do controlo da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral [41]

A generalização da utilização dos meios de comunicação no âmbito laboral suscita novos problemas jurídicos relacionados com a salvaguarda da privacidade, já que o empregador tem a possibilidade de controlar os dados e conteúdos transmitidos através da utilização de telefones, correio eletrónico e internet, existindo, portanto, um verdadeiro tratamento de dados pessoais dos trabalhadores.

Revela-se essencial garantir a harmonia entre a liberdade de gestão dos meios de trabalho e a reserva da intimidade da vida privada do trabalhador. O poder de direção (artigos 97º do Código do Trabalho) traduz-se no direito da entidade empregadora estabelecer os termos em que o trabalho deve ser prestado, tendo em conta o estipulado no contrato de trabalho. Este poder tem como limite os direitos e garantias dos trabalhadores. O Código do Trabalho contém disposições relativas à tutela dos direitos de personalidade do trabalhador no âmbito da relação laboral, nomeadamente o direito à reserva da intimidade da vida privada[42] e à proteção dos dados pessoais dos trabalhadores[43].

O artigo 22º, n.º 1 do Código do Trabalho consagra um princípio geral de confidencialidade das mensagens, não podendo o empregador aceder ao conteúdo das mensagens de natureza pessoal quando o trabalhador utilize os meios de comunicação disponibilizados pelo empregador. O n.º 2 do mesmo preceito concede legitimidade ao empregador para desenvolver regras de utilização dos meios de comunicação no local de trabalho, mas é importante estabelecer limites a essas regras para que as compressões aos direitos dos trabalhadores sejam proporcionais à finalidade prosseguida pelo empregador, não se revelando o tratamento excessivo e desproporcionado, de modo que os dados pessoais a serem tratados e os meios utilizados nesse tratamento, devem ser compatíveis com os

[41] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf (consultado a 4 julho 2014).

[42] Artigo 16º do Código do Trabalho.

[43] Artigo 17º do Código do Trabalho.

direitos e obrigações dos trabalhadores. Não se integram no âmbito do artigo 22º, n.º 2 do CT, as comunicações que o trabalhador efetue através do correio eletrónico, redes sociais ou de quaisquer contas pessoais, uma vez que o empregador está totalmente impedido de controlar a esfera privada daquele.

Num mundo cada vez mais tecnológico, em que os meios de comunicação fazem parte da rotina de trabalho, não é racional a proibição absoluta da utilização de telefones e telemóveis, do correio eletrónico e do acesso à internet para fins pessoais. Por isso, a entidade empregadora deve atribuir prioridade a metodologias de controlo de caráter genérico (que se revelam suficientes para cumprir os objetivos do controlo), afastando a consulta individualizada de dados pessoais. O acesso regular ao registo das comunicações efetuadas pelo trabalhador, além de desproporcionado, pode revelar-se ineficaz, por criar um clima de tensão no seio da empresa.

Impõem as disposições dos artigos 2º, 5º e 10º da LPD e também os artigos 106º e 107º do Código do Trabalho, que a entidade empregadora tem o dever de informação para com os trabalhadores, na medida em que os controlos das comunicações podem ser efetuados sem que o trabalhador deles se aperceba. Deve a entidade empregadora informar os trabalhadores sobre as regras de utilização dos meios de comunicação da empresa para fins privados, bem como o grau de tolerância admitido na sua utilização, as consequências de uma utilização indevida desses meios e a especificação dos métodos de controlo.

Os dados contidos nas comunicações privadas do trabalhador, por dizerem respeito à sua vida privada e por ser informação relativa a pessoa identificada ou identificável, enquadram-se no conceito de dados sensíveis (cf. artigo 3º, alínea a) e artigo 7º, n.º 1 da LPD). O tratamento de dados sensíveis é permitido se verificada alguma das circunstâncias prevista nos restantes números do artigo 7º. No caso em concreto, o fundamento de legitimidade para a permissão deste tipo de tratamento de dados sensíveis reside no Código do Trabalho, mais especificamente nos artigos 22º, n.º 2 e 97º, o que significa que a parte inicial do n.º 2 do artigo 7º da LPD atribui legitimidade para este género de tratamento, ao encontrar a sua condição de licitude nas referidas disposições do Código do Trabalho, uma vez que cabe ao empregador designar as regras de utilização dos meios de comunicação da empresa.

A escolha dos meios de controlo pelo empregador deve obedecer aos princípios da necessidade, suficiência, razoabilidade, proporcionalidade e boa-fé.

O artigo 20º do Código do Trabalho estatui a proibição de utilização de meios tecnológicos de vigilância pelo empregador para controlar o trabalhador. É inadmissível a utilização de sistemas que permitam visualizar ou monitorizar as ações do trabalhador no computador.

4.3.3.1. Os tratamentos de dados em particular

A. Princípios relativos ao controlo de dados de comunicações telefónicas e de dados de tráfego

A gravação de chamadas telefónicas, só pode ocorrer nos termos concretizados na Deliberação 629/2010, que trataremos mais adiante[44]. Este tratamento de dados apenas se admite para três finalidades específicas – prova da relação contratual, chamadas de emergência e monitorização da qualidade do atendimento – não sendo jamais admitido para finalidade de controlo do trabalhador (20º CT).

B. Princípios relativos ao controlo do correio eletrónico

Independentemente das regras definidas pelo empregador quanto à utilização do correio eletrónico para fins privados, este não pode abrir o correio eletrónico que se dirija ao trabalhador. Às profissões em que o sigilo e a confidencialidade são essenciais ao seu desempenho, como é o caso de médicos, advogados ou jornalistas, não é admissível qualquer tipo de controlo, pois seriam colocados em causa princípios constitucionais como a liberdade de imprensa (artigo 38º, n.º 2, alínea b) CRP).

O controlo do correio eletrónico deve ter como objetivo garantir a segurança do sistema e ser realizado de forma aleatória, e não permanente e sistemática, não devendo incluir a consulta do conteúdo das mensagens, uma vez que constitui um

[44] Questão analisada no ponto 4.5. (Tratamentos de dados na gravação de chamadas).

acesso não autorizado, extravasando a finalidade do tratamento. A necessidade de detetar vírus ou software malicioso não legitima a leitura do correio eletrónico do trabalhador.

Constatando o empregador que um determinado trabalhador faz uma utilização excessiva do correio eletrónico, aquele deverá avisá-lo e proceder ao controlo mediante meios alternativos e menos intrusivos. O acesso ao correio eletrónico deverá ser o último recurso e, caso suceda, terá de contar com a presença do trabalhador visado e, se possível, com um representante da comissão de trabalhadores ou de outra estrutura representativa dos mesmos. O acesso ao correio eletrónico do trabalhador com fundamento em ausência prolongada, deve ser devidamente fundamentado e do conhecimento do trabalhador visado.

C. Princípios relativos à internet

Cabe à entidade empregadora assegurar-se de que os trabalhadores estão devidamente informados e conscientes dos limites estabelecidos à utilização da internet para fins privados no local de trabalho e que conhecem as formas de controlo adotadas no seio da empresa.

O empregador deve optar por uma atuação preventiva, preferindo a criação de um sistema que impossibilite a navegação em websites cuja consulta não autoriza. Estando em causa a produtividade de um trabalhador, o controlo do mesmo deve ser feito através da contabilização do tempo médio de conexão e, perante a verificação de acessos excessivos, o trabalhador deve ser avisado. Se o trabalhador persistir no seu comportamento, poderá ser alvo de um processo disciplinar.

Mesmo nas situações em que o trabalhador utilize a internet no local de trabalho, desrespeitando as condições de utilização impostas pelo empregador, é absolutamente vedado o acesso ao perfil pessoal do trabalhador em redes sociais, uma vez que se afigura como um espaço de carácter pessoal ou mesmo íntimo.

4.4. Tratamento de dados de saúde

4.4.1 Tratamentos de dados efetuados no âmbito de estudos de investigação científica na área da saúde[45]

Os estudos de investigação efetuados na área da saúde seguem objetivos distintos e tratam categorias de informação bastante diversificadas e, dessa forma, os estudos podem assumir-se numa vertente observacional, epidemiológicos, retrospetivos e/ou prospetivos. Independentemente da forma que assumam, os estudos de investigação na área da saúde recaem sobre dados sensíveis (cf. artigo 7º, n.º 1 LPD) e, por esta razão, nos termos do artigo 28º, n.º 1, alínea a), estão sujeitos a controlo prévio por parte da CNPD e não poderão iniciar-se antes da obtenção da respetiva autorização.

Cabe à CNPD efetuar uma ponderação dos interesses em jogo, tendo em conta o princípio da proporcionalidade. Esta ponderação terá de se efetuar entre o direito à privacidade e à proteção dos dados pessoais, enquanto direito fundamental respeitante aos direitos, liberdades e garantias individuais, e o interesse público na investigação científica com consagração constitucional no capítulo dos direitos e deveres culturais, nomeadamente no artigo 73º, n.º 4 da CRP, verificando se o tratamento de dados se revela como o meio adequado para o fim visado. Não existe um direito à ciência, apenas uma obrigação estadual de incentivar a investigação científica.

Pelo facto de os dados alvo dos estudos de investigação na área da saúde terem a natureza de sensíveis, aplica-se o princípio da proibição do seu tratamento, sendo abertas exceções no artigo 7º, números 2, 3 e 4 da LPD. Nestes tratamentos, a legitimidade decorre do consentimento livre, específico, informado, expresso e escrito do titular, pela conjugação das disposições do artigo 3º, alínea h), artigo 7º,

[45] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/DEL227-2007-ESTUDOS-CLINICOS.pdf (consultado a 4 julho 2014).

n.º 2 da LPD e artigo 4º, n.º 3 da Lei n.º 12/2005, de 26 de janeiro,[46] relativa à informação genética pessoal e à informação de saúde.

A demonstração da obtenção do consentimento do titular cabe à entidade responsável pelo tratamento. Nos termos da definição do artigo 3º, alínea d) da LPD, pode assumir-se como responsável pelo tratamento qualquer das instituições referidas no artigo 2º da Lei n.º 125/99, de 20 de abril[47], que estabelece as normas que se aplicam às instituições que se dedicam à investigação científica. As unidades de saúde do Sistema Nacional de Saúde podem configurar-se como responsáveis por um tratamento de dados de saúde para fins de investigação científica.

Sempre que um estudo possa ser efetuado com recurso a dados anonimizados, o investigador deve privilegiar essa opção. Caso o estudo não possa efetuar-se nesses moldes, deve privilegiar-se a utilização de dados codificados. A utilização de dados de saúde para fins de investigação científica, apenas serão admitidos quando se verifique uma estrita necessidade da sua utilização, devendo a entidade responsável pelo tratamento justificar a necessidade de o estudo ser efetuado com recurso a dados identificados ou identificáveis.

Nos estudos de investigação, os dados podem ser recolhidos de forma direta junto do titular, por resposta a inquéritos/questionários ou de forma indireta através do médico assistente que os transmitirá ao investigador. No caso de recolha de amostras, devem ser adotadas técnicas pouco intrusivas e meios que preservem a dignidade da pessoa humana e a integridade física e moral das pessoas.

Quando a recolha dos dados pessoais não for efetuada por um profissional de saúde, têm de ser adotadas medidas que impeçam a visualização dos dados por pessoa não autorizada, bem como a fim de tornar segura a circulação da informação (cf. artigo 15º, n.º 1, alíneas b) e h) da LPD).

Nos estudos retrospetivos, aquando da escolha da amostra objeto de estudo, quando o estudo dependa da verificação de certos parâmetros, é imprescindível aceder a informação pré-existente que esteja na posse do estabelecimento de saúde ou do médico do titular dos dados. Nas situações em que é necessário aceder àquela

[46] Disponível em http://www.cnpd.pt/bin/legis/nacional/Lei12-2005.pdf (consultado a 4 julho 2014).

[47] Disponível em http://www.igf.min-financas.pt/inflegal/bd_igf/bd_legis_geral/Leg_geral_docs/DL_125_99.htm (consultado a 4 julho 2014).

informação, assume-se como *condição sine qua non* à realização do estudo, que a entidade responsável pelo tratamento solicite ao detentor dos dados pessoais que contacte os titulares para que estes concedam o seu consentimento para os seus dados integrarem o estudo a ser realizado.

A Lei n.º 12/2005, de 26 de janeiro, admite no n.º 6 do artigo 19º que "No caso de uso retrospetivo de amostras ou em situações especiais em que o consentimento das pessoas envolvidas não possa ser obtido devido à quantidade de dados ou de sujeitos, à sua idade ou outra razão comparável, o material e os dados podem ser processados, mas apenas para fins de investigação científica ou obtenção de dados epidemiológicos ou estatísticos."

Tratando-se de uma investigação científica em que a informação de saúde seja retirada de outros dados que não as amostras, não existindo consentimento do titular dos dados, a permissão para o tratamento desses dados pessoais deve ter em conta o interesse público subjacente à realização da investigação em questão, sendo que esse interesse público terá de ser comprovado não só pela entidade que acompanha cientificamente estas instituições, como pelo Ministério responsável pelas áreas em concreto (cf. artigo 11º, n.º 1, alínea a) e n.º 2 e artigo 12º da Decreto-Lei n.º 125/99, de 20 de abril).

Diferente será a utilização de dados de saúde para fins de investigação científica, no âmbito de teses académicas, uma vez que a responsabilidade pelo tratamento é do autor da tese e não se deve permitir a utilização desses dados pessoais sem o consentimento dos seus titulares, uma vez que uma pessoa individual dificilmente conseguirá adotar medidas de segurança adequadas a proteger os dados recolhidos. Nestes casos, os Comités de Ética das Universidades ou dos Hospitais podem responsabilizar-se pelo acompanhamento da investigação, atribuindo à pessoa individual meios adequados para o desenvolvimento do seu estudo. Deste modo, podem criar-se condições para que o tratamento de dados de saúde para fins de investigação científica, sem a prévia obtenção de consentimento dos titulares dos mesmos, seja admissível. Contudo, cada situação terá de ser analisada de forma casuística.

O direito de acesso aos dados de saúde deve ser exercido por intermédio do médico escolhido pelo titular dos dados, tal como dispõe o artigo 11º, n.º 5 da LPD e o artigo 3º, n.º 3 da Lei n.º 12/2005, de 26 de janeiro.

Caso o responsável pelo tratamento opte por contratar uma entidade externa para elaborar o estudo, essa prestação de serviços deve ser regida por um contrato ou ato jurídico que vincule as partes (cf. artigo 14º LPD).

Por regra, não pode haver comunicação de dados, contudo, nas investigações que envolvam vários centros de estudo, os dados pessoais podem ser comunicados entre esse centros, comunicação que deve ser do conhecimento do titular dos dados e que deve respeitar regras de segurança da informação.

4.4.1.1. Particularidades do consentimento

Ao longo do texto acima, muito nos referimos a diferentes formas de consentimento: livre, específico, informado, expresso e escrito. Neste ponto, cabe-nos explicar o significado de cada consentimento referido.

O consentimento é livre quando o titular dos dados pessoais não tem conhecimento de qualquer fator que condicione a formação da sua vontade no momento em que faz a sua declaração de consentimento. O consentimento diz-se específico por se reportar a um contexto factual em concreto. Referimo-nos a consentimento informado quando o titular dos dados conhece todos os elementos relevantes, para compreender o que se encontra subjacente ao tratamento de dados a realizar. É aqui que encontramos o dever de informação do responsável pelo tratamento, espelhado no direito de informação do titular dos dados do artigo 10º da LPD. O responsável pelo tratamento tem o dever de esclarecer o titular dos dados, certificando-se que este compreendeu o conteúdo do direito de informação. O consentimento informado é expressão dos princípios da transparência, da boa-fé e da lealdade.

Por sua vez, o consentimento expresso significa que o consentimento do titular dos dados não pode ser retirado de modo implícito de outras declarações que o mesmo haja feito, ou seja, o consentimento para ser expresso tem de ser prestado

para aquele tratamento de dados em específico. Por fim, o consentimento escrito deve constar de um texto escrito ou subscrito pelo titular.

4.4.2. Tratamentos de dados no âmbito de ensaios clínicos com medicamentos de uso humano [48]

A investigação científica assume um papel primordial no que se refere ao avanço da medicina e, inevitavelmente, a evolução das técnicas médicas para comprovarem a sua eficácia têm de recorrer à experimentação em seres humanos. Naturalmente, existem riscos associados a essa experimentação, que tem de se pautar não só por regras técnicas e científicas específicas, como tem de atribuir primazia à vida humana e à dignidade de cada indivíduo, respeitando exigências legais e éticas para a experimentação médica em seres humanos. Neste sentido impõe-se a Declaração de Helsínquia[49] datada de 1964, que se caracteriza por um conjunto de princípios éticos que regem a pesquisa com seres humanos.

Nos termos do artigo 6º, n.º 1, alínea c) da Lei n.º 46/2004, de 19 de agosto[50], daqui em diante designada de Lei dos Ensaios Clínicos (LEC), o direito à privacidade e à proteção dos dados pessoais afigura-se como a condição mínima de proteção dos participantes nos ensaios clínicos. A investigação em seres humanos só deve realizar-se quando a sua finalidade se assumir mais importante que os riscos e incómodos para o indivíduo, o que significa que o bem-estar dos participantes em ensaios clínicos deve ser sempre superior aos interesses prosseguidos pela ciência, princípios que encontram consagração na Declaração de Helsínquia, mais propriamente nos seus pontos 8 e 18 e também no artigo 3º da LEC.

A realização de ensaios clínicos inclui, inevitavelmente, o tratamento de dados pessoais sensíveis (cf. artigo 3º, alínea a) e artigo 7º, n.º 1 da LPD). Neste âmbito, os dados pessoais de saúde dos participantes têm necessariamente que ser objeto de

[48] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/DEL333-2007-ENSAIOS-CLINICOS.pdf (consultado a 4 julho 2014).

[49] Disponível em http://www.wma.net/en/30publications/10policies/b3/ (consultado a 4 julho 2014).

[50]Disponível em http://www.infarmed.pt/portal/page/portal/INFARMED/LEGISLACAO/LEGISLACAO_FARMACEUTICA_COMPILADA/TITULO_III/TITULO_III_CAPITULO_I/036-C_Lei_46_2004_1.%AAAlt.pdf (consultado a 4 julho 2014).

tratamento para que se cumpra a finalidade prosseguida pelos ensaios clínicos, porém, o tratamento desses dados deve restringir-se ao necessário para a prossecução do ensaio. As restantes categorias de dados pessoais sensíveis elencadas no artigo 7º, n.º 1 da LPD, como os dados relativos à vida sexual, vida privada e origem racial ou étnica, devem apenas ser utilizados nos ensaios clínicos quando respeitem o artigo 5º, n.º 1, alínea c). Já os dados relativos às convicções filosóficas ou políticas, filiação partidária ou sindical e à fé religiosa não podem ser tratados no âmbito dos ensaios clínicos.

A condição de legitimidade do tratamento de dados pessoais dos participantes em ensaios clínicos encontra-se no consentimento livre, específico, informado, expresso, escrito, datado e assinado pelos mesmos, o que resulta de disposições conjugadas da Lei de Proteção de Dados (artigo 3º, alínea h) e artigo 7º, n.º 2, 2ª parte), da Lei n.º 12/2005, de 26 de janeiro (artigo 4º, n.º 3) e ainda da Lei dos Ensaios Clínicos (artigo 2º, alínea o). Tal como dispõe o artigo 6º, nº 2 da LEC, o consentimento é livremente revogável, a todo o tempo, de forma expressa ou tácita.

Quando os participantes nos ensaios clínicos sejam menores ou incapazes de exprimirem o seu consentimento, este depende dos seus representantes legais, o qual deve refletir a vontade presumível do menor ou incapaz e, além disso, "(…) considerar o desejo explícito do participante que seja capaz de formar uma opinião (…)"[51]. Atingindo o menor a maioridade ou o incapaz alcance a plena capacidade de exercício dos seus direitos no decurso do ensaio, o responsável pelo tratamento deve obter o consentimento escrito e expresso destes participantes. Caso o participante não se encontre em condições de prestar o seu consentimento por escrito, este pode ser prestado oralmente, desde que na presença de duas testemunhas, tal como estipula o artigo 2º, alínea o) da Lei dos Ensaios Clínicos, sendo da competência da Comissão de Ética pronunciar-se sobre o procedimento de obtenção do consentimento (cf. artigo 20º, n.º 3, alínea g) LEC).

A obrigação de obtenção do consentimento pertence ao investigador. [52]

A Lei dos Ensaios Clínicos contempla uma secção referente aos responsáveis pela realização do ensaio, sendo eles o promotor, o investigador e o monitor,

[51] Artigo 7º, alíneas a) a c) e artigo 8º, n.º 2, alíneas a) a c) da Lei dos Ensaios Clínicos.

[52] Artigo 10º, alínea c) da Lei dos Ensaios Clínicos.

estando as suas competências estabelecidas do artigo 9º ao artigo 11º, respetivamente.[53] Segundo o artigo 14º, nº 1 da mencionada lei, é solidária[54] a responsabilidade do investigador com o promotor, uma vez que cabendo ao primeiro atos que complementam a atividade do promotor, aquele responderá independentemente de culpa por todos os incidentes no decurso do tratamento dos dados pessoais. Tanto o monitor como o investigador podem considerar-se como subcontratantes nos termos do artigo 3º, alínea e) da LPD, devendo ser respeitado o estipulado no artigo 16º e no artigo 14º, n.º 3 da LPD, respeitantes ao tratamento de dados pessoais por subcontratantes.

Perante os participantes no ensaio clínico, perante as entidades de tutela e fiscalização e perante terceiros, a entidade responsável é o promotor, independentemente da responsabilidade solidária com o investigador, já que é aquele que determina a finalidade do tratamento e o modo como este se vai realizar.

O consentimento prestado para se ser participante num ensaio clínico, não pode confundir-se com o consentimento prestado para o tratamento de dados pessoais, na medida em que o consentimento exigido para o tratamento de dados pessoais sensíveis tem de ser expresso e escrito e não se pode extrair de forma implícita do consentimento para participação num ensaio clínico.

Aquando do tratamento de dados podem existir vários centros de ensaio envolvidos e a comunicação de dados pessoais dos participantes entre esses centros não se considera uma comunicação de dados a terceiros, mas apenas uma circulação de dados pessoais entre centros de ensaio que têm uma entidade responsável em comum.

[53] O promotor é a entidade responsável, na medida em que determina a finalidade e os meios do tratamento, enquanto o investigador é quem pratica os atos típicos da entidade responsável, como é o caso da prestação do dever de informação, da obtenção do consentimento dos participantes, entre outras competências descritas no citado preceito.

[54]Existe solidariedade nas relações entre o promotor e o investigador, no sentido em que havendo lugar a imputação de responsabilidade por uma atuação danosa, qualquer um deles responde por essa atuação.

4.4.3. Tratamentos de dados com a finalidade de prescrição eletrónica de medicamentos e gestão do processo clínico

No âmbito da prescrição eletrónica de medicamentos e de gestão do processo clínico dos utentes existe comunicação de dados para a Administração Central do Sistema de Saúde (ACSS), no que se refere ao Sistema de Conferência de Faturas de Medicamentos, comunicação esta já concedida pela Autorização n.º 36/99[55] e pela Autorização n.º 38/2001[56]. Esta comunicação terá de ocorrer sem transmissão de dados pessoais dos utentes.

Nas autorizações emitidas pela CNPD, distinguem-se três tipos de perfis de acesso à informação. O perfil "médico" pode registar e aceder a toda a informação, pertencendo-lhe, em exclusivo, a capacidade de prescrever medicamentos. O perfil "enfermeiro" contempla a visualização da informação necessária para a prática dos atos de enfermagem, assim como o registo sobre os medicamentos prescritos pelo primeiro e sobre a administração dos mesmos. Já o utilizador com o perfil "administrativo" tem acesso às informações estritamente necessárias para o exercício da sua atividade, tendo conhecimento das consultas agendadas e efetuadas, altas e dados de faturação.

Os tratamentos de dados pessoais com a finalidade de prescrição eletrónica de medicamentos e gestão do processo clínico, são realizados nos termos do artigo 7º, n.º 4 da LPD. [57]

Relativamente aos dados automatizados, o sistema deve garantir uma separação lógica entre os dados de saúde e os restantes dados pessoais (cf. artigo 15º, n.º 3 da LPD). O sistema informatizado deverá permitir o acesso à informação

---

[55] Autorização disponível em http://www.cnpd.pt/bin/decisoes/Aut/10_36_1999.pdf (consultado a 4 julho 2014).

[56] Autorização disponível em http://www.cnpd.pt/bin/decisoes/Aut/10_38_2001.pdf (consultado a 4 julho 2014).

[57] "O tratamento dos dados referentes à saúde e à vida sexual, incluindo os dados genéticos, é permitido quando for necessário para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados ou tratamentos médicos ou de gestão de serviços de saúde, desde que o tratamento desses dados seja efetuado por um profissional de saúde obrigado a sigilo ou por outra pessoa sujeita igualmente a segredo profissional, seja notificado à CNPD, nos termos do artigo 27º, e sejam garantidas medidas adequadas de segurança da informação."

de acordo com os diferentes perfis de utilizador, com distintos níveis de acesso à informação, devendo ser atribuída uma palavra-passe a cada utilizador.

4.4.4. Tratamentos de dados com a finalidade de gestão de utentes

Na sua maioria, os dados dos utentes dos serviços prestados no âmbito da gestão de utentes, assumem-se como dados sensíveis, uma vez que se referem à saúde e à vida privada, impondo o artigo 7º, n.º 1 da LPD, por norma, a proibição do tratamento dos dados com esta natureza. Nas situações de gestão de utentes, o fundamento de legitimidade para o tratamento de dados pessoais referentes à vida privada resulta do n.º 2 do referido preceito, ou seja, do consentimento dos titulares dos dados.

Nos termos do artigo 10º do aludido diploma, o titular dos dados tem de ser informado sobre a identidade do responsável pelo tratamento, bem como a finalidade do tratamento e ainda sobre as condições em que poderá exercer o direito de acesso e de retificação dos seus dados.

Atendendo à natureza sensível dos dados objeto de tratamento, o responsável pelo tratamento deverá adotar as medidas de segurança adequadas a proteger os dados pessoais dos riscos inerentes ao tratamento (cf. artigo 15º da LPD), sendo que os dados referentes à saúde devem estar separados dos restantes dados pessoais.

4.5. Tratamentos de dados na gravação de chamadas[58]

A presente Deliberação veio revogar a Deliberação n.º 922/2009[59] adotada pela CNPD, na qual se estabeleciam as condições gerais para os tratamentos de dados pessoais decorrentes da gravação de chamadas efetuadas numa de três vertentes possíveis: relação contratual, emergência e prestação de serviços de promoção, informação e apoio aos consumidores e utentes através de centros

[58] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/DEL629_2010.pdf (consultado a 4 julho 2014).

[59] Disponível em http://www.cnpd.pt/bin/orientacoes/DEL_922_2009.pdf (consultado a 4 julho 2014).

telefónicos de relacionamento, também designados de call centers. As especificidades associadas às prestações de serviço dos call centers originaram a elaboração do Decreto-Lei n.º 134/2009, de 2 de junho[60], que estabeleceu no seu artigo 9º uma obrigação legal de manter a gravação de chamadas efetuadas pelo consumidor por 90 dias (n.º 2). No entanto, o Decreto-Lei n.º 72-A/2010, de 18 de junho, procedeu à revogação do artigo 9º do Decreto-Lei n.º 134/2009, de 2 de junho[61] e, como tal, existiu a necessidade de atualizar o conteúdo da Deliberação revogada.

Teremos de atribuir especial atenção ao facto de no âmbito do tratamento de dados decorrente de gravações de chamadas, os dados pessoais do próprio trabalhador cuja atividade seja o contacto telefónico com os clientes, serem objeto de tratamento.

Estipula a Lei n.º 41/2004, de 18 de agosto[62] o princípio geral do sigilo das comunicações (cf. artigo 4º, n.º 1), admitindo exceções a esta regra no corpo do restante artigo 4º. [63] Por estarem sujeitos a sigilo, os dados pessoais tratados no âmbito da gravação de chamadas incidem sobre dados sensíveis, pois estamos perante dados da vida privada (cf. artigo 7º, n.º 1 da LPD). Nas situações de emergência, estão em causa dados relativos à saúde e até mesmo dados relativos à

[60] Disponível em http://dre.pt/pdf1sdip/2009/06/10600/0345203454.pdf (consultado a 4 julho 2014).

[61] Revogação prevista no artigo 92º do Decreto-Lei n.º 72-A/2010, de 18 de junho.

[62] Disponível em http://www.anacom.pt/render.jsp?contentId=944401 (consultado a 4 julho 2014).
Esta lei aplica-se aos tratamentos de dados pessoais no contexto dos serviços de comunicações eletrónicas.

[63]

Artigo 4.º
Inviolabilidade das comunicações eletrónicas

1—As empresas que oferecem redes e ou serviços de comunicações eletrónicas devem garantir a inviolabilidade das comunicações e respetivos dados de tráfego realizadas através de redes públicas de comunicações e de serviços de comunicações eletrónicas acessíveis ao público.

2 — É proibida a escuta, a instalação de dispositivos de escuta, o armazenamento ou outros meios de interceção ou vigilância de comunicações e dos respetivos dados de tráfego por terceiros sem o consentimento prévio e expresso dos utilizadores, com exceção dos casos previstos na lei.

3 — O disposto no presente artigo não impede as gravações legalmente autorizadas de comunicações e dos respetivos dados de tráfego, quando realizadas no âmbito de práticas comerciais lícitas, para o efeito de prova de uma transação comercial nem de qualquer outra comunicação feita no âmbito de uma relação contratual, desde que o titular dos dados tenha sido disso informado e dado o seu consentimento.

4 — São autorizadas as gravações de comunicações de e para serviços públicos destinados a prover situações de emergência de qualquer natureza.

vida sexual. Estes tratamentos carecem, assim, de controlo prévio por parte da CNPD (cf. artigo 28º, n.º 1, alínea a) da LPD).

A empresa terá de informar os seus trabalhadores de que as chamadas efetuadas serão gravadas, a fim de respeitar o disposto no artigo 106º do Código do Trabalho, direito de informação que terá de ser realizado através de um dos meios previstos no artigo 107º do mesmo diploma e que não se confunde com o direito de informação consagrado no artigo 10º da Lei de Proteção de Dados. Respeitados estes dois preceitos, o empregador atuará de acordo com os princípios da transparência e da boa-fé.

Princípio que também deverá ser particularmente observado é o princípio da proporcionalidade, pois estamos perante tratamentos de dados em que se afigura fundamental ponderar os interesses dos intervenientes na relação contratual, não só na relação entre a empresa e os titulares dos dados, como na relação entre a empresa e os respetivos trabalhadores.

As gravações de chamadas efetuadas no âmbito de uma relação contratual, têm como finalidade fazer prova das transações comerciais ocorridas entre o responsável pelo tratamento e os titulares dos dados pessoais e de quaisquer outras comunicações realizadas no âmbito da relação contratual que os liga. As gravações de chamadas no âmbito de situações de emergência, têm como finalidade fazer prova do cumprimento das obrigações relativas ao serviço de emergência. Por sua vez, as gravações de chamadas no âmbito da monitorização da qualidade do atendimento, têm como finalidade controlar a qualidade do serviço.

Relativamente às condições de legitimidade para os tratamentos de dados dos clientes, quando os tratamentos decorram da gravação de chamadas efetuadas no âmbito de uma relação contratual, esse tratamento de dados é permitido desde que o dever de informação aos titulares dos dados tenha sido cumprido e estes tenham dado o seu consentimento prévio, expresso e inequívoco para o tratamento. Quando os tratamentos de dados decorram da gravação de chamadas efetuadas no âmbito de situações de emergência, o fundamento de legitimidade encontra-se no artigo 7º, n.º 2 da Lei de Proteção de Dados. Se os tratamentos decorrerem da gravação de chamadas no âmbito da monitorização da qualidade do atendimento, o

consentimento dos titulares dos dados constitui condição de legitimidade para o tratamento.

Quanto ao tratamento de dados dos trabalhadores, é imprescindível existir uma ponderação entre o direito da entidade empregadora fixar os termos em que o trabalho deve ser prestado e os direitos dos trabalhadores cuja atividade contempla o contacto telefónico com clientes ou utentes. Essa ponderação assume-se particularmente relevante nas situações em que o tratamento incide sobre a monitorização da qualidade do atendimento, uma vez que poderá estar em causa uma avaliação de desempenho dos trabalhadores, sendo proibida a utilização de meios de vigilância à distância no local de trabalho que tenham a finalidade de controlar o desempenho profissional do trabalhador. [64] As gravações de chamadas com o intuito de controlar os trabalhadores, afigura-se uma medida desproporcionada que entraria em colisão com a privacidade dos trabalhadores, uma vez que o empregador pode utilizar para essa finalidade outros instrumentos menos intrusivos da privacidade dos mesmos. O trabalhador deve ter ao seu dispor outro meio que não seja alvo de gravação para realizar comunicações pessoais (cf. artigo 22º do Código do Trabalho).

No que se refere ao responsável pelo tratamento de dados, este depende da finalidade inerente à gravação de chamadas. No tratamento de dados pessoais decorrente da gravação de chamadas efetuadas no âmbito da relação contratual, o responsável pelo tratamento é a entidade com quem o titular dos dados tem uma relação contratual. No tratamento de dados decorrente da gravação de chamadas efetuadas no âmbito de situações de emergência, o responsável pelo tratamento é o serviço público a quem compete prestar auxílio nestas situações, ou seja, o Instituto Nacional de Emergência Médica (INEM) [65]. No tratamento de dados decorrente da gravação de chamadas efetuadas no âmbito da monitorização da qualidade do atendimento, o responsável pelo tratamento é a entidade empregadora.

---

[64] Artigo 20º, n.º 1 Código do Trabalho.

[65] Informação disponível em http://dre.pt/pdf1sdip/2003/07/173A00/43924398.pdf (consultado a 4 julho 2014).
Parte inicial do preâmbulo do Decreto-Lei n.º 167/2003, de 29 de julho:
"Ao Instituto Nacional de Emergência Médica, abreviadamente designado por INEM, cabe a função de coordenação do Sistema Integrado de Emergência Médica (SIEM), no quadro do qual se inclui toda a atividade de urgência/emergência (…)"

Face à finalidade dos tratamentos em causa, não se afigura pertinente a existência de comunicação dos dados recolhidos. No que se refere à interconexão desses dados, ainda que regra geral não sejam de admitir, podem existir situações em que se justifiquem, tendo de ser apreciada casuisticamente e dependendo da verificação da sua adequação, necessidade e não excessividade em relação à finalidade do tratamento. A possibilidade de existirem call centers em países exteriores à União Europeia tem também de ser apreciada casuisticamente, de forma a que se entenda se o país para o qual os dados serão transferidos, assegura um nível de proteção adequado aos mesmos.

4.6. Tratamentos de dados com a finalidade de cessão de créditos

A cessão de créditos encontra consagração no Código Civil nos artigos 577º a 588º e assume-se como uma figura em que o credor originário é substituído, mantendo-se os restantes elementos da relação obrigacional, ou seja, a obrigação mantém-se inalterada, alterando-se simplesmente a titularidade do credor da obrigação. Esta é, portanto, uma forma de transmissão de crédito, mediante a celebração de um negócio jurídico.

A cessão de créditos pode realizar-se independentemente do consentimento ou da colaboração do devedor, tal como consta do artigo 577º, n.º 1 do Código Civil, uma vez que este é apenas um terceiro relativamente à cessão, sendo as figuras principais a do cedente e a do cessionário.[66]

A cessão de créditos tem como efeito a transmissão do crédito, como se disse, do credor originário para um novo credor, sendo que essa transmissão abrange tudo o que esteja inerente ao crédito, com exceção das garantias que não se possam dissociar da pessoa do cedente.

Os dados pessoais objeto de tratamento estão sujeitos a sigilo bancário, conforme resulta do disposto no artigo 78º do Decreto-Lei n.º 298/92, de 31 de dezembro, que estipula o Regime Geral das Instituições de Crédito e Sociedades

[66] Por cedente entenda-se o credor originário (que transmite o crédito) e por cessionário o credor substituto (o terceiro para quem o crédito é transmitido).

Financeiras[67]. Por se referirem a dados da vida privada (cf. artigo 7º, n.º 1 da LPD), estão sujeitos a controlo prévio por parte da CNPD (cf. artigo 28º, n.º 1, alínea a) da LPD).

O fundamento de legitimidade para que estes tratamentos de dados pessoais sejam permitidos, reside no artigo 7º, n.º 2 da LPD, ou seja, quando se imponham motivos de interesse público importante ou quando o titular dos dados tiver dado o seu consentimento para o tratamento.

Comum às autorizações emitidas pela CNPD no domínio da cessão de créditos, são os dados pessoais do devedor a que a entidade cessionária terá acesso, como é o caso do nome, os seus contactos, número de identificação fiscal, número de cartão de cidadão, bilhete de identidade ou de autorização de residência, estado civil, dados relativos ao contrato, valores do crédito em dívida, a taxa de juro aplicável, os pagamentos efetuados, o montante original da dívida e dados do processo judicial. Estes dados serão recolhidos do devedor e, caso seja necessário, do cônjuge e dos avalistas.

Os dados pessoais referidos serão entregues à cessionária que se comprometerá a aceder a estes dados na medida do necessário ao exercício dos direitos de crédito resultantes da cessão e no contexto do estipulado no contrato de cessão de crédito.

Igualmente importantes são o direito de informação ao titular dos dados, como estipulado no artigo 10º da LPD e a adoção de medidas de segurança nos termos dos artigos 14º e 15º do mesmo diploma.

67

Artigo 78.º
Dever de segredo

1 - Os membros dos órgãos de administração ou de fiscalização das instituições de crédito, os seus empregados, mandatários, comitidos e outras pessoas que lhes prestem serviços a título permanente ou ocasional não podem revelar ou utilizar informações sobre factos ou elementos respeitantes à vida da instituição ou às relações desta com os seus clientes cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços.

2 - Estão, designadamente, sujeitos a segredo os nomes dos clientes, as contas de depósito e seus movimentos e outras operações bancárias.

3 - O dever de segredo não cessa com o termo das funções ou serviços.

4.7. Videovigilância

4.7.1. Tratamentos de dados por meio de videovigilância segundo a opinião 4/2004, de 11 de fevereiro, do Grupo de Trabalho do Artigo 29º[68]

O objetivo prosseguido pelo Grupo de Trabalho com este parecer é o de contribuir para a harmonização da aplicação das medidas nacionais adotadas nos termos da Diretiva n.º 95/46/CE, no domínio da videovigilância. Nos últimos anos, tem-se assistido a uma crescente utilização de sistemas de videovigilância, sendo que esta utilização pode assumir diversas finalidades, como é o caso da proteção de pessoas, proteção de bens, motivada por interesses públicos, para deteção e controlo de infrações ou como meio de prova da prática de ilícitos criminais.

Se existem casos em que o recurso a câmaras de videovigilância é obrigatório[69], são ainda mais os casos em que se utiliza essa tecnologia de forma desmedida, por não se afigurar proporcional e adequada às circunstâncias em concreto e por a legislação aplicável não ser observada. A informação recolhida por sistemas de videovigilância refere-se a pessoas identificadas ou identificáveis que foram captadas pelos sistemas enquanto circulavam nos locais abrangidos pelos mesmos. No entanto, pelo facto de um indivíduo ser filmado por uma câmara de videovigilância, não pode significar uma privação aos direitos e liberdades do mesmo, embora a sua privacidade se veja diminuída.

A Diretiva n.º 95/46/CE não tem aplicação em determinados domínios, como disposto no artigo 3º, n.º 2. Desde logo, não se aplicará ao tratamento de dados de som e imagem relacionados com os domínios da segurança pública, no desempenho de atividades do Estado no âmbito do direito penal ou em atividades cujo âmbito de aplicação do direito penal não abranja. [70] Por outro lado, a Diretiva não se aplicará

---

[68] Disponível em http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf (consultado a 4 julho 2014).

[69] Casos de utilização obrigatória de sistemas de videovigilância são os postos de abastecimento de combustível, as instituições de crédito e sociedades financeiras, farmácias, grandes superfícies comerciais e também estabelecimentos onde se exiba, compre ou venda metais preciosos e obras de arte.

[70] Considerando 16 da Diretiva.

às situações em que o sistema de videovigilância se destine exclusivamente ao exercício de atividades pessoais ou domésticas.[71] Por último, nos termos do artigo 9º da Diretiva, nos tratamentos de som e imagem com finalidades jornalísticas ou de expressão literária ou artística a Diretiva terá aplicação se os Estados-Membros assim o entenderem. [72]

No parecer, o Grupo de Trabalho alertou para três situações em que os dados relativos a pessoas identificadas ou identificáveis são sempre dados pessoais para efeitos de aplicação da Diretiva. A primeira situação consiste na utilização de imagens num sistema de videovigilância, mesmo que as imagens não contenham caraterísticas específicas de um indivíduo. Numa segunda situação, os dados serão sempre pessoais ainda que os rostos dos indivíduos não tenham sido filmados, mas existam outro tipo de informações como matrículas de automóveis. Por último, os dados serão sempre considerados dados pessoais independentemente do equipamento usado, do suporte de armazenamento dos dados e das ferramentas de comunicação.

O responsável pelo tratamento deve tomar as medidas adequadas para assegurar que o sistema de videovigilância que pretende implementar está de acordo com os princípios de proteção de dados, para que o tratamento de dados pessoais seja lícito (cf. artigo 6º, n.º 1, alínea a) e para não existirem alusões desnecessárias à privacidade.[73]A adequação e proporcionalidade do tratamento de dados à finalidade para que foram recolhidos leva-nos a concluir que os sistemas de videovigilância só poderão ser utilizados em situações em que o recurso a estes sistemas seja efetivamente necessário. Segundo o princípio da proporcionalidade, a utilização destes sistemas é permitida quando outras medidas de proteção e segurança sejam claramente insuficientes tendo em conta a finalidade prosseguida.

---

[71] Considerando 12 da Diretiva.

[72] Considerando 17 da Diretiva.

[73] Na nota de rodapé n.º 15 do parecer em análise, consta um exemplo de uma alusão desproporcionada ao direito à privacidade, senão vejamos. Neste exemplo, que corresponde a uma situação da vida real, um cliente de um banco foi assaltado e foi-lhe levado o seu cartão de multibanco, sendo que o ladrão utilizou o cartão do cliente para retirar dinheiro da conta do mesmo numa caixa automática. Existia uma câmara de videovigilância a filmar a caixa automática. Posto isto, o cliente solicitou acesso às gravações dessa câmara, a fim de obter imagens do assalto a que tinha sido sujeito. O acesso às imagens foi negado, alegadamente por uma questão de privacidade.

Compete ao responsável pelo tratamento minimizar as consequências e danos para os titulares dos dados que podem resultar do tratamento dos mesmos, além de dever o primeiro dar primazia aos tratamentos de dados que recorram a dados anónimos e, se possível, não utilizar dados pessoais.

4.7.2. Princípios sobre o tratamento de dados por videovigilância segundo a Deliberação n.º 61/2004, de 19 de abril, da CNPD[74]

O Decreto-Lei n.º 231/98, de 22 de julho[75] que regulava o exercício da atividade de segurança privada, previa no artigo 12º que as entidades vocacionadas para a prestação de serviços de segurança privada podiam recorrer a sistemas de videovigilância para as auxiliar no desempenho das suas funções. Todavia, o Acórdão n.º 255/02, de 12 de junho de 2002[76], proferido pelo Tribunal Constitucional, declarou a inconstitucionalidade do artigo 12º do Decreto-Lei n.º 231/98, logo, deixou de existir fundamento de legitimidade para a utilização de sistemas de videovigilância no desempenho da atividade de segurança privada.

O Tribunal Constitucional fixou jurisprudência no sentido de que os sistemas de videovigilância, por restringirem direitos, liberdades e garantias dos cidadãos, apenas podem ser utilizados quando a lei assim o estipular ou mediante autorização dos titulares dos dados. Nas situações em que os sistemas possam ser utilizados, as restrições que imponham aos direitos fundamentais dos indivíduos terão de limitar-se ao estritamente necessário para assegurar os direitos ou interesses que estejam subjacentes a essa utilização. Compete à CNPD, no caso concreto, verificar a admissibilidade do tratamento, tendo em conta o artigo 35º, n.º 3 da CRP e o artigo 7º, números 2 e 3 da LPD.

---

[74] Deliberação disponível em http://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf (consultado a 4 julho 2014).

[75] Disponível em http://dre.pt/pdf1sdip/1998/07/167A00/35153522.pdf (consultado a 4 julho 2014).

[76] Disponível em http://www.tribunalconstitucional.pt/tc/acordaos/20020255.html (consultado a 4 julho 2014).

Na sequência da declaração de inconstitucionalidade, foi publicado o Decreto-Lei n.º 35/2004, de 21 de Fevereiro[77] que veio afirmar a relevância da atividade de segurança privada no nosso quotidiano e consagrou novamente, desta vez no artigo 13º, a possibilidade de utilização de sistemas de videovigilância no âmbito da mesma.

A já nossa conhecida Lei de Proteção de Dados, impõe que os responsáveis pelo tratamento procedam à notificação do mesmo (cf. artigo 27º), assim como que observem os princípios de proteção de dados e as condições de licitude para o tratamento dos dados, dispostas na Secção I do Capítulo II da LPD. Os dados pessoais tratados através de sistemas de videovigilância são dados sensíveis, nos termos do artigo 7º, n.º 1 da LPD, por integrarem o conceito de vida privada.

Existem casos em que a própria lei impõe ou admite a utilização de sistemas de videovigilância, como é o caso dos recintos de competições desportivas[78], dos estabelecimentos de fabrico e armazenagem de produtos explosivos[79]ou quando, de modo geral, " (…) particulares exigências inerentes à natureza da atividade o justifiquem."[80]

A implementação de sistemas de videovigilância encontra-se muitas vezes associada à prevenção da criminalidade e, nestes casos, o fundamento de legitimidade para o tratamento e recolha dos dados decorre do artigo 8º, n.º 2 da LPD. Nestas situações pretende-se dissuadir a eventual prática de ilícitos criminais, mas não se afigura digno que as pessoas que frequentem lugares alvo de videovigilância estejam sob suspeita, logo, o direito de informação do artigo 10º da LPD cumpre aqui um papel importante, uma vez que todos os locais que possuam estes sistemas têm de conter claramente a referência à existência dos sistemas.[81] Deste modo, os sistemas de videovigilância, por estarem incumbidos de proteger

[77] Disponível em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=283&tabela=leis (consultado a 4 julho 2014).

[78] Disponível em http://dre.pt/pdf1sdip/1998/08/178A00/37313737.pdf (consultado a 4 julho 2014). Artigo 11º da Lei n.º 38/98, de 4 de agosto.

[79] Disponível em http://dre.pt/pdf1sdip/2002/05/114A00/45584579.pdf (consultado a 4 julho 2014). Artigo 22º, n.º 2 e n.º 3, alínea b) do Decreto-Lei n.º 139/2002, de 17 de maio.

[80] Artigo 20º, n.º 2 do Código do Trabalho.

[81] Questão analisada no ponto 5.8.4., notas de rodapé 125 e 126.

pessoas e bens, podem afigurar-se como um meio de prevenção e dissuasão de práticas criminais e, caso esta finalidade falhe, as imagens captadas pelos mesmos podem vir a servir como meio de prova nos termos da lei processual penal.[82] Nestas situações, aplica-se o artigo 11º, n.º 2 da LPD, nos termos do qual os pedidos de acesso às imagens deverão ser dirigidos à CNPD, que avaliará as condições concretas do pedido de acesso. Fora destes casos, a visualização das imagens só será possível se os titulares dos dados exercerem o direito de acesso, nos termos do artigo 11º da LPD, tendo o responsável pelo tratamento de assegurar que os dados de terceiros não sejam expostos aquando da visualização das imagens no âmbito do direito de acesso.

4.7.3. Processo de contraordenação por realização de tratamento de dados pessoais decorrente da instalação e utilização ilegítima de equipamento de videovigilância

O processo[83] que aqui discutiremos resulta da notificação de um tratamento de dados pessoais através de um sistema de videovigilância instalado num prédio, que obteve a Autorização n.º 3940/2012, de 9 de maio[84], emitida pela CNPD. Esta instaurou um processo de contraordenação ao condomínio do prédio em questão, tendo-o condenado ao pagamento de uma coima e ordenado o bloqueio do sistema de videovigilância.

Fundamentou o arguido que o sistema não violava a vida privada dos condóminos, pelo facto de este apenas registar movimentos nas partes comuns do edifício e não proceder ao tratamento de dados da vida privada. Fundamentou também que estava em causa a segurança dos condóminos e a instalação do sistema obteve a aprovação da sua maioria, não podendo "(…) ficar reféns da decisão de um

[82] Problemática discutida no ponto 5.8.3. (Utilização como meio de prova de imagens captadas por sistemas de videovigilância não legalizados).

[83] Acórdão do Tribunal da Concorrência, Regulação e Supervisão, de 21 de outubro de 2013 (Processo n.º 140/13.6YUSTR).

[84] Autorização disponível em http://www.cnpd.pt/bin/decisoes/Aut/10_3940_2012.pdf (consultado a 4 julho 2014).

condómino (…)", tendo o sistema por finalidade a prevenção, segurança e prova de condutas criminosas.

Impõe-se esclarecer o sucedido para uma melhor compreensão do caso aqui discutido. O condomínio do prédio em causa deliberou em assembleia de condóminos instalar um sistema de videovigilância, motivado pela vaga de assaltos que existiam na zona circundante e pela avançada idade da maioria dos condóminos. No entanto, nessa assembleia não participou um dos condóminos que, posteriormente, informou a administração do condomínio que não aprovava a instalação do sistema e exigiu que o mesmo fosse retirado. Todavia, os restantes condóminos entenderam que a instalação do sistema foi aprovada por unanimidade entre os presentes na assembleia e que, além disso, possuíam autorização da CNPD para o efeito e que não existia violação da vida privada, uma vez que as câmaras se encontravam direcionadas para zonas comuns do prédio (porta principal, porta secundária, porta e janelas da garagem). Porém, consta da Autorização emitida pela CNPD que " A instalação de sistemas de videovigilância só poderá ocorrer se for consentida por todos os condóminos e arrendatários dos imóveis à data da instalação daqueles meios."

O acórdão refere que o direito à vida privada não é sinónimo de direito à imagem, tratando-se de dois direitos diferenciados. Enquanto o direito à vida privada pode ser infringido de diversas formas não necessariamente ligadas à recolha da imagem de um indivíduo, o direito à imagem pode ser desrespeitado fora do âmbito da vida privada, podendo suceder que ambos os direitos sejam infringidos simultaneamente.

Não só a Constituição da República Portuguesa consagra o direito à reserva da intimidade da vida privada[85], como encontra consagração na lei civil[86] e na lei penal [87], o que significa claramente que o ordenamento jurídico português atribui uma proteção transversal à vida privada. O conceito de vida privada não é facilmente

[85] Artigo 26º, n.º 1 CRP.

[86] Artigo 80º do Código Civil.

[87] Artigo 190º e seguintes do Código Penal.

definível, uma vez que é uma noção vaga, que poderá incluir inúmeras realidades e, portanto, torna-se impreciso. [88]

Frequentemente discutida é a contraposição entre o direito à vida privada e o direito à segurança. Além de este assumir uma importância fulcral na vida de todos os indivíduos, uma vez que a sensação de segurança ou a falta dela tem consequências nas ações das pessoas e no seu quotidiano, não incumbe apenas ao Estado assegurá-la, pois é também incumbência de todos os cidadãos praticar ações que ajudem a dotar um determinado espaço de alguma segurança. O direito à segurança é garantia de outros direitos fundamentais e, como tal, não se deve considerar irrelevante quando comparado com outros direitos.

O artigo 7º, números 2, 3 e 4 da LPD operam como uma restrição do direito à segurança no âmbito da videovigilância, uma vez que não contém nenhum elemento que nos conduza à sua prevalência sobre o direito à vida privada. As restrições que sejam executadas por lei a direitos, liberdades e garantias têm de respeitar três pressupostos para serem legítimas. Em primeiro lugar, essas restrições legais só se podem verificar para acautelar outros direitos ou interesses constitucionalmente protegidos. Em segundo lugar, o princípio da proporcionalidade tem de estar preenchido nas suas três vertentes: o princípio da adequação, segundo o qual as restrições legais têm de se afigurar como o meio adequado para prosseguir os fins visados; O princípio da necessidade exige que essas medidas sejam necessárias aos fins visados, no sentido em que estes não se conseguiriam atingir por outros meios menos onerosos para os direitos, liberdades e garantias; O princípio da proporcionalidade em sentido estrito impõe que as medidas restritivas devem assumir-se justas, não se afigurando desproporcionais e excessivas, tendo em conta as finalidades prosseguidas. O artigo 7º da LPD respeita o princípio da proporcionalidade nas suas três vertentes: a proibição de tratamentos de dados relativos à vida privada e as possíveis derrogações a essa regra afiguram-se idóneas à tutela deste direito, pois impede que seja desrespeitado. É também uma medida necessária, uma vez que a videovigilância apresenta uma elevada capacidade de dano para a vida privada. O facto de as exceções à regra da proibição de tratamento serem

[88] Questão discutida no ponto 5.6.1. (Tratamento de dados sensíveis).

limitadas abrange todas as situações que, em princípio, justificam a compressão do direito à vida privada.

Por último, as restrições legais a direitos, liberdades e garantias não podem resultar no aniquilamento de nenhum direito fundamental, devendo, no entanto, ter-se em conta a necessidade de salvaguardar outros direitos constitucionalmente protegidos. No caso do direito à segurança, serão poucos os casos em que este direito será inadmissivelmente comprimido, uma vez que não só a eficácia da videovigilância não é absoluta nem comprovada, como a própria segurança das imagens recolhidas não se encontra garantida, como ainda se pode recorrer a meios menos ofensivos da vida privada para garantir a segurança. Todavia, a regra proibitiva consagrada no artigo 7º, n.º 1 da LPD deverá ser afastada quando, casuisticamente, o direito à vida privada aniquilar o conteúdo essencial do direito à segurança.

Concluiu o tribunal que embora as câmaras de videovigilância instaladas no edifício se encontrassem direcionadas para as áreas comuns, tinham aptidão para recolher informação relativa à vida privada dos condóminos, nomeadamente, as horas a que entravam e saiam, as pessoas que os acompanhavam, entre outras informações suscetíveis de serem captadas. Afirmou que " (…) não é possível o exercício em simultâneo dos dois direitos conflituantes nos termos reivindicados pelos envolvidos e o conteúdo essencial do direito à segurança dos condóminos que consentiram na instalação das câmaras não fica aniquilado."

O facto de os condóminos se sentirem inseguros devido à criminalidade de que já tinham sido alvo e às práticas criminosas a que assistiam nas zonas circundantes ao seu prédio, demonstram a potencial situação de insegurança que viviam, contudo, poderiam recorrer a outros meios menos intrusivos da vida privada, como a instalação de alarmes ou o recurso a um vigilante, não se afigurando proporcional, no caso em concreto, recorrer àquela que deverá ser a última medida a adotar.

Considera o tribunal que o consentimento da maioria dos condóminos é irrelevante, na medida em que existe um condómino que manifestou a sua oposição à instalação do sistema e, em concreto, o direito à vida privada deste sobrepõem-se ao direito à segurança e à propriedade dos demais, não ficando o conteúdo essencial

destes direitos aniquilado, uma vez que os condóminos podem recorrer a outras medidas.

Assim, conclui-se pela não verificação de qualquer exceção do artigo 7º da LPD, mantendo-se a condenação do condomínio no pagamento da coima e no bloqueio do sistema de videovigilância instalado.

4.8. Gabinete de Atendimento ao Público: questões suscitadas

Embora tenha estado apenas uma semana no Gabinete de Atendimento ao Público (GAP), foi a experiência mais enriquecedora que tive durante o estágio, no sentido em que tive a oportunidade de tomar contacto com as dúvidas que os cidadãos possuem no domínio da proteção de dados, dúvidas essas que tocaram as matérias mais diferenciadas, tendo ficado com uma noção alargada das temáticas que a proteção de dados abrange e tendo também me apercebido que os quatro meses e meio de estágio foram suficientes para conhecer o principal das questões suscitadas na Comissão Nacional de Protecção de Dados, mas que muitos outros aspetos ficaram por abordar.

Neste ponto, vou expor algumas questões que foram colocadas e que achei interessantes para debater no ponto relativo à análise crítica das atividades desenvolvidas, por reclamarem uma maior atenção e tem sobretudo que ver com a videovigilância. As questões que decidi individualizar são as seguintes:

1) Câmaras instaladas em ginásios que funcionam em horários noturnos, com a finalidade de segurança das instalações e das pessoas que o frequentam;
2) Controlo de trabalhadores por meio de câmaras de videovigilância;
3) Utilização de imagens captadas por câmaras de videovigilância não autorizadas para efeitos de prova em processo criminal;
4) Controlo oculto por meio de videovigilância.

5. Análise crítica das atividades desenvolvidas

Pretendendo-se com este relatório de estágio dar a conhecer as atividades nele desenvolvidas e atendendo ao facto de no Ponto 4, relativo à descrição das mesmas, as variadas temáticas terem sido explanadas de forma completa e compreensível, não se afigura necessário no presente ponto repetir as ideias já referidas, preferindo, deste modo, analisar questões relativamente às quais é necessária uma explicação adicional para uma melhor compreensão dos dados pessoais e tudo o que os envolve, nomeadamente no que se refere a conceitos básicos.

5.1. Legislação de proteção de dados pessoais: evolução e relevância na proteção da privacidade

No âmbito internacional, o reconhecimento do direito à privacidade remonta ao ano de 1948, mais propriamente à Declaração Americana dos Direitos e Deveres do Homem[89], cujo artigo 5º consagra que "Toda a pessoa tem direito à proteção da lei contra ataques abusivos à sua honra, reputação e à vida privada e familiar". A 10 de dezembro de 1948, é aprovada a Declaração Universal dos Direitos Humanos[90], na qual se reconhecem direitos inerentes à própria personalidade de todo o Homem, de que é exemplo o respeito pela sua privacidade. O seu artigo 12º constitui a base para a elaboração de convenções posteriores, como é o caso do Pacto Internacional sobre Direitos Civis e Políticos (16 de dezembro de 1966).[91]

A nível internacional são dois os instrumentos que assumem especial relevância no que se refere ao reconhecimento da necessidade de proteção da privacidade enquanto direito fundamental: a Convenção do Conselho da Europa

[89] Disponível em http://www.cidh.oas.org/Basicos/Portugues/b.Declaracao_Americana.htm (consultado a 4 julho 2014).

[90] Disponível em http://www.dre.pt/comum/html/legis/dudh.html (consultado a 4 julho 2014).

[91] Disponível em http://www.cidadevirtual.pt/cpr/asilo2/2pidcp.html (consultado a 4 julho 2014).

para a Proteção de Dados Pessoais Automatizados, de 28 de janeiro de 1981[92] (Convenção n.º 108) e as Linhas Diretrizes da OCDE[93] sobre a proteção da vida privada, de 23 de setembro de 1980. [94]

A privacidade é considerada um direito fundamental na maioria dos países, embora seja diversamente encarada, havendo de se operar uma distinção entre os ordenamentos jurídicos europeus e os ordenamentos jurídicos norte-americanos, pois enquanto nos primeiros a privacidade se encontra relacionada com os direitos de personalidade, nos segundos deriva do conceito de propriedade.

5.1.1. Na Europa

No contexto europeu, o desenvolvimento da proteção do direito à privacidade surgiu nos anos 40. Foi e continua a ser na Europa que sempre se revelou uma preocupação enorme na defesa deste direito, com o reconhecimento de uma posição assumidamente protetora através dos instrumentos normativos e das observações que têm sido elaboradas acerca da proteção da privacidade.

Acresce que o projeto europeu pretende a criação de um ordenamento jurídico com princípios e ideias partilhadas por todos os Estados-Membros, existindo, portanto, um esforço de harmonização das legislações dos mesmos, o que torna a sua atuação mais fácil, mais coesa e consequentemente mais forte, embora cada país opere a proteção da privacidade e dos dados pessoais nos trâmites disciplinados pela sua legislação.

Com a criação do Conselho da Europa, foi elaborada em 1950 a Convenção Europeia dos Direitos Humanos, que consagrou um conjunto de direitos a serem

---

[92] Disponível em http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm (consultado a 4 julho 2014).

[93] A Organização para Cooperação e Desenvolvimento Económico (OCDE) é uma organização internacional que agrupa os países mais industrializados que se reúnem para trocar informações e definir políticas com o objetivo de maximizar o crescimento económico e o desenvolvimento dos países membros.

[94] As Linhas Diretrizes da OCDE, sob a forma de recomendações, consagram princípios sobre a recolha de dados, cujo âmbito de aplicação pode ser ampliado, se os Estados assim o entenderem. Os princípios consagrados são oito: princípio da limitação em matéria de recolha, princípio da qualidade dos dados, princípio da especificação das finalidades, princípio da limitação da utilização, princípio das garantias de segurança, princípio da transparência, princípio da participação individual e princípio da responsabilidade.

respeitados e assegurados pelos Estados-Membros, sendo o primeiro texto europeu a fazê-lo. [95]

A 26 de setembro de 1973 foi adotada a Resolução R (73) 22 sobre proteção da vida privada das pessoas singulares face aos bancos de dados eletrónicos no setor privado. Um ano depois, foi adotada a Resolução R (74) 29, relativa à proteção da vida privada das pessoas singulares perante os bancos de dados eletrónicos no setor público. Estas Resoluções pretendiam influenciar os legisladores nacionais a adotarem ideias comuns no que se refere ao tratamento automatizado de dados pessoais.

A partir de 1980, a Organização para a Cooperação e Desenvolvimento Económico, de agora em diante designada OCDE, aprovou um conjunto de linhas diretrizes referentes à proteção da privacidade e fluxo internacional de dados pessoais e à segurança dos sistemas de informação e redes.

Devido à rápida evolução tecnológica, existiu a necessidade de se elaborar uma Convenção que abordasse a proteção de dados pessoais e a transferência além fronteiras dos mesmos, não esquecendo que em simultâneo teria de se reforçar a proteção dos direitos dos cidadãos, nomeadamente, a proteção da vida privada, pelo facto de a comunicação de dados passar a ser uma realidade, o que requer medidas de segurança adicionais na proteção dos dados. Assim, surgiu, a 28 de janeiro de 1981, a Convenção n.º 108[96] (Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal). A Convenção entrou em vigor a 1 de outubro de 1985 e visou implementar um nível mínimo de proteção dos dados pessoais no âmbito europeu, estando na liberdade de cada Estado atribuir uma proteção mais elevada aos mesmos, ou seja, os Estados podiam alargar a proteção dos dados pessoais além do consagrado nas disposições da Convenção (artigo 11º), assim como podiam entender não aplicar a Convenção a determinadas categorias de dados. Em Portugal, foi com a publicação da Lei n.º 10/91, de 29 de abril, que se criaram condições para que a Convenção fosse ratificada. A Convenção

[95] A Convenção Europeia dos Direitos Humanos inspirou-se na Declaração Universal dos Direitos Humanos, no entanto, enquanto a primeira detém a obrigatoriedade própria dos tratados internacionais, o mesmo não acontece com a segunda.

[96] Disponível em http://www.cnpd.pt/bin/legis/internacional/Convencao108.htm (consultado a 4 julho 2014).

é um dos instrumentos fundamentais da proteção de dados pessoais, pois nela foram consagrados princípios fundamentais que vieram a integrar a Diretiva n.º 95/46/CE.

Desde a adoção da Convenção n.º 108 que se tem verificado um desenvolvimento tecnológico bastante notório, uma vez que no nosso quotidiano somos utilizadores em grande escala de meios eletrónicos, informatizados e de produtos que se encontram em constante evolução e, por isso, o Conselho da Europa vai-se adaptando às novas realidades, mediante a elaboração de Recomendações dirigidas a diferentes setores, que complementam o disposto na Convenção. Constituindo um passo muito importante na história da União Europeia, a Carta dos Direitos Fundamentais da União Europeia[97], datada de dezembro de 2000, consagra inúmeros direitos fundamentais, nomeadamente no artigo 7º (respeito pela reserva da vida privada) pretendendo-se com este preceito assegurar que a pessoa possa desenvolver livremente a sua personalidade, protegendo-se de intromissões de terceiros e também no artigo 8º (conceito de proteção de dados).

Tendo em conta a disparidade de normas legais existentes entre os Estados-Membros da União Europeia sobre proteção de dados pessoais, foi elaborada a Diretiva n.º 95/46/CE, de 24 de outubro, referente à livre circulação de dados pessoais entre os Estados-Membros, caraterizando-se por ser o primeiro texto normativo que consagrou tal proteção, não se assumindo exclusivamente como um instrumento protetor dos direitos das pessoas, mas como uma forma de estipular quais as situações em que os dados são suscetíveis de serem comunicados e de que forma podem os mesmos ser transmitidos, estabelecendo limites à livre circulação de informação de caráter pessoal. Esta Diretiva tem uma importância fulcral não só no âmbito europeu, como no âmbito internacional, uma vez que estabelece um regime de transferência dos dados pessoais, não só entre Estados-Membros, como entre estes e países que não pertencem à União Europeia.

Posteriormente à Diretiva n.º 95/46/CE, surgiu a Diretiva n.º 97/66/CE, de 15 de dezembro, relativa ao tratamento de dados pessoais no setor das telecomunicações que acabou derrogada pela Diretiva n.º 2002/58/CE, de 12 de

[97] Disponível em http://www.europarl.europa.eu/charter/pdf/text_pt.pdf (consultado a 4 julho 2014).

julho, que, por sua vez, foi alterada pela Diretiva n.º 2006/24/CE, de 15 de março, cujo âmbito de aplicação se destina aos serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações.

5.1.2. Nos Estados Unidos

"Nos EUA verificam-se mais casos sobre violação da privacidade do que em qualquer outro ordenamento jurídico" refere TERESA ALEXANDRA COELHO MOREIRA ("A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação", 2010). Com o 11 de setembro de 2001 existiu o que podemos apelidar de ponto de viragem no que se refere à compressão do conteúdo do direito à privacidade nos Estados Unidos que, anteriormente a este acontecimento, já sucedia de um modo geral.

Nos Estados Unidos da América interligam-se regulamentos federais e estaduais com medidas de autoregulação. De facto, não existe uma entidade que zele pela aplicação dos princípios fundamentais da proteção da privacidade do cidadão o que potencia a vulnerabilidade dos cidadãos às intromissões na sua vida privada.

Assim, as políticas de privacidade seguidas pelos EUA e pela UE seguem orientações distintas. Enquanto nos EUA se prefere uma abordagem sectorial, uma fusão de regulamentação com autoregulamentação, na UE existe legislação mais abrangente, com destaque para a Diretiva n.º 95/46/CE. Tendo em conta ambos os regimes, é fácil constatar que, sendo que o regime dos EUA não cumpria os níveis adequados de proteção que eram exigidos pela Diretiva europeia, estaríamos perante grandes adversidades no que se refere às transferências de dados pessoais e à sua proteção.

A solução surgiu com o desenvolvimento de um conjunto de princípios a respeitar pelas empresas norte-americanas: o Safe Harbor Agreement[98]. Trata-se de

[98] Mais informações em http://export.gov/safeharbor/eu/eg_main_018365.asp (consultado a 4 julho 2014).

São sete os "Safe Harbor Principles", em português "princípios do porto seguro":

1. Princípio do aviso prévio: as empresas ficam obrigadas não só a notificar os titulares dos dados sobre as informações recolhidas a seu respeito e dos fins a que se destina essa recolha, como também a fornecer informação sobre o modo como os titulares dos dados podem contactar a empresa, caso necessitem de o fazer. Este princípio exige que a informação seja formulada de forma concisa e recorrendo a uma linguagem clara e percetível pelo destinatário da mesma;

um programa a ser utilizado exclusivamente por empresas dos EUA que recebam dados pessoais com origem na UE. Cada empresa norte-americana que se registe no programa, sujeita-se a uma avaliação de conformidade com um variado leque de normas consideradas adequadas nos termos do artigo 25º da Diretiva relativa à transferência de dados pessoais para países terceiros. Isto significa que o Safe Harbor Agreement não é mais que um instrumento de certificação de organizações norte-americanas, que visa garantir a observância das regras europeias úteis a uma prática comercial saudável entre aquelas e as empresas europeias, no respeito pelos direitos fundamentais dos indivíduos quanto à circulação sem fronteiras dos seus dados pessoais.

5.1.3. Em Portugal

Foi no artigo 35º da Constituição da República Portuguesa (CRP) que se atribuiu uma particular importância ao tratamento de dados pessoais, reflexo da transposição da Diretiva n.º 95/46/CE que, aquando da quarta revisão constitucional (1997) e também com o surgimento da Lei de Proteção de Dados (Lei n.º 67/98, de 26 de outubro), se deu um passo importante na regulamentação da proteção de dados em Portugal.

O artigo 35º da CRP foi objeto de importantes alterações legislativas, operadas pelas revisões constitucionais de 1982, de 1989 e de 1997 e carateriza-se por ser um

2. Princípio da escolha: cabe aos titulares dos dados a faculdade de escolher se os seus dados podem ou não ser transmitidos a terceiros ou se podem ser utilizados para outra finalidade que não aquela para a qual foram recolhidos;
3. Princípio relativo a transferências para terceiros: é imprescindível garantir que os dados não são transferidos por uma empresa que siga os princípios do porto seguro para outra empresa que não ofereça a proteção adequada;
4. Princípio do acesso aos dados pessoais: direito atribuído ao titular dos dados pessoais de conhecer quais as suas informações pessoais que são detidas por uma dada empresa;
5. Princípio da segurança dos dados: as empresas norte-americanas devem tomar precauções para proteger os dados pessoais de perdas, mau uso, divulgação, alteração e destruição não autorizadas;
6. Princípio da integridade dos dados: os dados devem assumir-se relevantes para os fins a que se destina o seu uso, não sendo possível à empresa tratar os dados de forma incompatível com os fins para os quais foram recolhidos;
7. Princípio da aplicação: para que seja assegurado o cumprimento dos princípios do porto seguro, as empresas devem disponibilizar mecanismos de recurso que permitam aos indivíduos a reparação de eventuais danos no tratamento dos seus dados pessoais.

direito de personalidade[99],visando proteger os cidadãos dos perigos para a sua privacidade inerentes à utilização da informática. Este revela-se o preceito principal no que se refere à regulação da proteção da privacidade. Todavia, a Constituição atribui um papel relevante nesta matéria a outros artigos, como é o caso do artigo 26º, relativo ao direito à reserva da intimidade da vida privada e do artigo 34º, referente à inviolabilidade do sigilo da correspondência e de outros meios de comunicação privada.

O artigo 26º da CRP contempla direitos de personalidade, pelo facto de todos eles se encontrarem ligados à proteção do núcleo da vida de qualquer cidadão, ou seja, aos seus direitos pessoais. No n.º 1 do referido preceito, encontramos consagrado o direito à imagem, este que é um direito que inclui a faculdade que cada um tem de consentir ou não que seja fotografado ou de ver uma imagem sua exposta. Similar ao direito à imagem é o direito à palavra, no âmbito do qual não podem ser escutadas nem gravadas conversas privadas, sem que para tal exista consentimento do visado. Atendendo ao conteúdo do direito à palavra, não só o indivíduo tem direito à sua voz, no sentido de esta não ser registada ou divulgada, como tem direito a decidir quem são os destinatários da palavra.

Para COSTA ANDRADE, o direito à palavra e o direito à imagem correspondem a expressões diretas da personalidade, assumindo-se como bens jurídicos pessoais para o Direito Penal.[100]

No n.º 1 in fine, bem como no n.º 2 encontramos a consagração do direito à reserva da intimidade da vida privada e familiar que se analisa em dois direitos menores. Desde logo, o direito a impedir o acesso de terceiros a informações sobre a vida privada e familiar e, por outro lado, o direito a não ver divulgadas essas informações. O direito à inviolabilidade do domicílio e da correspondência (artigo

[99] Os direitos de personalidade traduzem-se em direitos supra legais, uma vez que são hierarquicamente superiores a todos os outros direitos, por serem imprescindíveis à esfera jurídica de qualquer pessoa. Estes representam poderes jurídicos inerentes a todos os cidadãos adquiridos com o nascimento e, por isso, são direitos gerais, já que são direitos de todos os cidadãos. Os direitos de personalidade são irrenunciáveis, logo, não está na disponibilidade dos titulares renunciar aos mesmos, além de que são protegidos contra qualquer ofensa ilícita, nos termos do artigo 70º do Código Civil.
Os direitos de personalidade são, assim, poderes jurídicos inerentes a todas as pessoas, por força do seu nascimento. Nas palavras de CARLOS ALBERTO DE MOTA PINTO "É um círculo de direitos necessários; um conteúdo mínimo e indispensável da esfera jurídica de cada pessoa" (Teoria Geral do Direito Civil, 2012, p. 209).

[100] Citado por Acórdão do Supremo Tribunal de Justiça de 28-09-2011 (Processo n.º 22/09.6YGLSB.S2)

342º do CP) funciona como garante da reserva da vida privada. O artigo 26º, n.º 2 demonstra a preocupação com a existência de uma garantia do direito à reserva da intimidade da vida privada e familiar. Este assume-se como um direito de personalidade que goza de proteção no âmbito civil e também no âmbito penal. Para o ordenamento jurídico civil, a sua proteção encontra-se no artigo 80º do Código Civil, enquanto para o ordenamento jurídico-penal a sua proteção realiza-se mediante o preenchimento dos tipos de ilícito que se encontram estipulados nos artigos 190º a 198º do Código Penal.

Já no que se refere à inviolabilidade do domicílio e da correspondência, constitucionalmente consagrada no artigo 34º, estamos perante bens jurídicos fundamentais na ordem jurídica portuguesa, como a dignidade da pessoa humana e a liberdade individual, relevante para a autodeterminação da personalidade de cada um. Traduz-se num direito essencial à manutenção da privacidade. Este direito é autónomo do direito à reserva sobre a intimidade da vida privada, apesar de com ele se interligar. Inerente a este direito encontramos a liberdade de qualquer pessoa efetuar comunicações quando e do modo que entender.

O direito ao segredo da correspondência visa proteger bens jurídicos fundamentais, como a privacidade e a dignidade da pessoa humana, embora admita algumas restrições, conforme resulta do n.º 4 do referido preceito. Este direito abrange toda e qualquer forma de comunicação privada.

A Constituição qualifica o direito ao domicílio e o sigilo das comunicações como invioláveis, no entanto, é uma inviolabilidade que admite restrições. Deve entender-se por domicílio o local onde se habita, seja ele permanente ou não.[101] A violação do domicílio não se dá somente com a entrada de alguém sem consentimento na habitação de uma determinada pessoa, mas também com a utilização de meios eletrónicos que permitam a intromissão na vida privada dos moradores. O domicílio é um espaço de individualidade da pessoa, onde a mesma poderá desenvolver livremente a sua personalidade e por esta razão considera-se "(…) o domicílio como projeção espacial da pessoa e a correspondência como

[101] Um quarto de hotel considera-se domicílio para efeitos de aplicação deste princípio.

exteriorização da própria pessoa".[102] O consentimento dos indivíduos é *condição sine qua non* da entrada de terceiros nos seus domicílios, com exceção dos casos de mandado judicial ou das situações em que o estado de necessidade o justifique.

O direito ao sigilo da correspondência e de outros meios de comunicação abarca todas as espécies de correspondência, desde o correio eletrónico à carta, das encomendas ao telefone, entre outras. No âmbito normativo deste preceito não se incluem aquelas informações que se destinam a outras pessoas de um modo geral e implica que terceiros que tenham acesso à informação não a divulguem, ou seja, a proteção desta norma opera-se não só em relação a quem viole o sigilo da correspondência, mas também em relação a terceiros que por qualquer razão tiveram acesso à informação, não podendo estes divulgá-la.

Por sua vez, o artigo 35º abrange a proteção dos cidadãos perante o tratamento de dados pessoais informatizados, não só na sua vertente de recolha, mas também nas vertentes de utilização e transmissão e encontra-se relacionado com a dignidade da pessoa humana e com o direito de autodeterminação informativa. Este tem como consequência a existência de direitos que serão explicados num ponto autónomo[103], como é o caso do direito de acesso, do direito à contestação, do direito à atualização e do direito à eliminação e carateriza-se por ser uma faculdade inerente a cada indivíduo de controlar a utilização dos seus dados pessoais. Este é um direito contra a intromissão de terceiros nos dados pessoais de determinada pessoa, cabendo ao titular dos mesmos decidir quais os dados que pretende manter alheios ao conhecimento de terceiros.

O direito à autodeterminação informativa não é uma mera garantia à reserva da vida privada, mas sim um direito fundamental que permite ao indivíduo opor-se à recolha e difusão dos seus dados pessoais.

Apesar de a proteção de dados pessoais no ordenamento jurídico português ter encontrado o seu fundamento no artigo 35º da CRP, não significou que a proteção dos dados pessoais informatizados se encontrasse cabalmente resolvida. Era necessário um imperativo próprio que preenchesse as lacunas que se

[102] GOMES CANOTILHO E VITAL MOREIA - *Constituição da República Portuguesa Anotada*; Volume I; p. 541.

[103] Analisados no ponto 5.4. (Direitos dos titulares dos dados).

verificavam, ao ponto de o Tribunal Constitucional ter declarado inconstitucionalidade por omissão nesta matéria.[104]Deste modo, surgiu a Lei de Proteção de Dados que transpôs para o ordenamento jurídico português a Diretiva n.º 95/46/CE e que tem aplicação aos tratamentos de dados pessoais operados quer por meios automatizados, quer por meios não automatizados, não se aplicando aos tratamentos de dados pessoais realizados por uma pessoa individual no contexto de interesses exclusivamente pessoais. [105] Novidade é a aplicação desta lei aos mecanismos de captação, tratamento e difusão de sons e imagens, que se traduzam na identificação de indivíduos, o que tem um alcance bastante vasto e engloba diversos tratamentos de dados. Uma das suas importantes consagrações foi a criação da Comissão Nacional de Proteção de Dados.

Já a Lei n.º 69/98, de 28 de outubro, procedeu à transposição da Diretiva n.º 97/66/CE, e veio complementar a Lei de Proteção de Dados, no entanto, foi revogada pelo Decreto-Lei n.º 41/2004, de 18 de agosto que concretizou também ele a transposição da Diretiva n.º 2002/58/CE que regula a proteção de dados pessoais no setor das comunicações eletrónicas.

5.2. Medidas de segurança no tratamento de dados

Nos termos do disposto no início do corpo do artigo 14º da Lei de Proteção de Dados, compete ao responsável pelo tratamento assegurar que este é efetuado com todas as garantias de segurança. Conforme resulta do n.º 1 do referido artigo, a segurança do tratamento inclui não só medidas que visem salvaguardar a informação, mas também medidas que protejam a integridade dos dados e a acessibilidade de pessoas não autorizadas aos mesmos.

---

[104] Acórdão 182/89 do Tribunal Constitucional.

[105] Segundo o artigo 4º, n.º 2 da LPD, esta não se aplica aos tratamentos de dados num âmbito exclusivamente pessoal ou doméstico, o que significa que, por exemplo, um indivíduo que quer instalar em sua casa um sistema de videovigilância que não capta via pública nem propriedade de terceiros e que não se destine a vigiar funcionários, não terá de notificar a instalação desse sistema, salvaguardando-se que deverá, independentemente disso, respeitar o direito de informação e o período de conservação dos dados.
O mesmo sucede com a Diretiva de proteção de dados (cf. nota de rodapé 72).

As medidas de segurança das informações assumem duas vertentes: física e lógica. Da segurança física fazem parte o alarme de intrusão, o acesso reservado às informações, bem como a localização dos equipamentos em locais de acesso restrito, entre outras medidas, enquanto na segurança lógica podemos destacar o acesso à informação mediante a utilização de palavra-passe ou de outra forma de autenticação igualmente segura, a transmissão de dados cifrados, entre outras medidas. A dotação do processo de tratamento de dados com palavra-passe de acesso às informações, assim como o acesso restrito de pessoas às instalações ou a adoção de sistemas de alarme, configuram-se medidas mínimas para que se possa considerar a existência de medidas de segurança aptas a salvaguardar as informações em tratamento.

Quando o tratamento incida sobre dados pessoais sensíveis ou quando se refiram a suspeitas de atividades ilícitas, infrações penais e contraordenações, respetivamente consagrados nos artigos 7º e 8º da LPD, a lei impõe ao responsável pelo tratamento a adoção de medidas de segurança de caráter especial[106]. A adequação da medida de segurança ao tratamento do dado em concreto, deve aferir-se tendo em conta o grau de sensibilidade que a informação possui. No caso de se verificar a circulação desses dados, consiste uma medida adequada que estes sejam encriptados, segundo o disposto no artigo 15º, n.º 4. Por outro lado, os dados de saúde devem encontrar-se separados dos restantes dados pessoais como estipula o n.º 3 do mesmo preceito.

Quando as informações estejam contidas num sistema informatizado, deve este estar estruturado de acordo com os diferentes utilizadores e com a acessibilidade da informação a cada um deles, devendo ser atribuída uma palavra-passe a cada utilizador. Essas palavras-passe devem ser periodicamente alteradas. Por outro lado, a informação não pode de modo algum ser acedida por pessoas que não tenham autorização para as conhecer e, por isso, caso exista um utilizador do sistema que tenha deixado de poder aceder às informações, o perfil desse utilizador deve ser eliminado.

Quanto aos dados contidos em suporte de papel, as medidas de segurança a adotar pelo responsável pelo tratamento terão de assegurar um nível de segurança

[106] Cf. artigo 15º da LPD.

idêntico ao que se verifica nos sistemas informatizados, impedindo que as informações sejam facilmente acessíveis e manuseadas por parte de quem não tem esses privilégios.

Cabe ao responsável pelo tratamento, não só a adoção de medidas de segurança, como o efetivo resultado dessas medidas.

5.3. Responsável pelo tratamento de dados

Segundo a definição proposta no artigo 3º, alínea d) da LPD, configurar-se-á como responsável pelo tratamento "a pessoa singular ou coletiva (…) que determine as finalidades e os meios de tratamento dos dados pessoais (…)". A obrigação de notificação do tratamento de dados contemplada no artigo 27º da LPD será de quem assumir a qualidade de responsável face ao tratamento de dados pessoais em concreto.

A responsabilidade pelo tratamento terá de ser individual, ou seja, esta estará incumbida a uma entidade ou pessoa, apenas sendo de admitir que a responsabilidade pelo tratamento seja partilhada por mais do que uma entidade nas situações em que não se verifique a possibilidade de averiguar a responsabilidade individualmente.

Muitas das obrigações do responsável pelo tratamento têm correspondência com os direitos dos titulares dos dados dispostos nos artigos 10º a 13º da LPD.
O responsável pelo tratamento tem ainda o dever de colaboração estipulado no artigo 24º da LPD que consiste na obrigação de prestar as informações que a CNPD lhe solicite, permitir a realização de inspeções aos ficheiros que contêm dados pessoais e ainda facultar documentos relacionados com o tratamento de dados pessoais.

5.4. Direitos dos titulares dos dados

5.4.1. Direito ao esquecimento

O direito ao esquecimento visa permitir a qualquer indivíduo solicitar que determinada informação sobre si seja eliminada, o que pressupõe que no decorrer do prazo de conservação dos dados, seja possível identificar os seus titulares (artigo 5º, n.º 1, alínea e) da LPD). Este direito tem implicações com o princípio do consentimento e com o princípio da finalidade, na medida em que nos termos do primeiro, para que se verifique um tratamento de dados pessoais, o titular destes terá de consentir previamente para que se opere a recolha, armazenamento e tratamento dos seus dados. Por outro lado, o princípio da finalidade impõe que os dados recolhidos sejam mantidos e utilizados de acordo com a finalidade que motivou a sua recolha. Assim, quando os dados pessoais de determinada pessoa não estejam a ser utilizados dentro das finalidades da recolha, pode o seu titular invocar direito ao esquecimento para que se verifique a remoção dos seus dados.

5.4.2. Direito à curiosidade

O direito à autodeterminação informativa é o fundamento para a existência do direito à curiosidade. Enquanto o direito de informação se prende com o direito do titular dos dados conhecer as finalidades subjacentes ao tratamento dos mesmos, o responsável pelo tratamento, bem como outras informações estipuladas no artigo 10º da LPD, o direito à curiosidade prende-se com o facto de o titular dos dados saber se uma determinada entidade possui dados relacionados consigo.

5.4.3. Direito de informação

O direito de informação encontra-se estipulado no artigo 10º da LPD e afirma-se como uma condição de licitude do tratamento de dados pessoais, uma vez que quando o titular dos dados desconheça que o tratamento está a ser efetuado,

então pode considerar-se que o tratamento não é lícito, aplicando-se o capítulo da Lei de Proteção de Dados relativo à tutela administrativa e jurisdicional. [107]

Nos termos do artigo 10º, n.º5, o direito de informação pode ser afastado se existir uma disposição legal neste sentido ou mediante Deliberação da CNPD, quando estejam em causa motivos relacionados com segurança, investigação criminal ou ainda em tratamentos de dados com finalidades estatísticas ou de investigação científica em que informar o titular dos dados se revele impossível ou desproporcionado.

O direito de informação no regime de proteção de dados pessoais é um direito essencial, corolário dos princípios da lealdade, boa-fé e transparência.

5.4.4. Direito de acesso

Estabelecido no artigo 11º da LPD, carateriza-se por permitir ao titular dos dados ter acesso aos mesmos, não sendo condição para o seu exercício que o titular justifique a sua intenção ao exercê-lo. O direito de acesso pode ser exercido de forma direta, isto é, diretamente junto do responsável pelo tratamento ou ainda de forma indireta, sendo que neste caso, o direito de acesso terá de ser exercido mediante um terceiro, como é o caso da CNPD. [108]

5.4.5. Direito de retificação e atualização

O titular dos dados pode exigir do responsável pelo tratamento que corrija e/ou atualize os seus dados. Este direito evita violações ao princípio da exatidão e atualização dos dados. Disposto no artigo 11º, n.º 1, alínea d), o direito de retificação é uma decorrência do artigo 5º da LPD, mais propriamente da alínea d) do n.º 1, princípio inerente à verificação da qualidade dos dados objeto de tratamento.

[107] Ver ponto 5.9. (Consequências do desrespeito pelas normas de proteção de dados).

[108] Cf. artigo 11º, números 2, 3 e 5 da LPD.

Uma vez incumprido o dever de retificação e atualização, competência do responsável pelo tratamento, incorre este numa contraordenação prevista e punível pelo artigo 38º, n.º 1, alínea b) da LPD.

Os direitos de acesso e retificação, tal como o direito de informação, assumem-se como direitos fundamentais ao regime da proteção de dados, com consagração no artigo 35º, n.º 1 da Constituição, sendo que os primeiros possuem um papel primordial na verificação dos princípios da adequação, pertinência e exatidão dos dados pessoais.

5.4.6. Direito de apagamento ou bloqueio dos dados

O titular dos dados pode, com fundamento no artigo 11º, n.º 1, alínea d), impelir o responsável pelo tratamento a apagar ou bloquear os seus dados pessoais.

5.4.7. Direito de não ficar sujeito a uma decisão individual automatizada

Consagrado no artigo 13º da LPD, consiste numa proibição de tomada de decisão baseada exclusivamente num tratamento automatizado de dados pessoais. Por outras palavras, não é proibida a tomada de decisão com base em tratamentos automatizados de dados. O que se proíbe é que essa tomada de decisão se fundamente exclusivamente em tratamentos automatizados.

5.4.8. Direito de oposição

O direito de oposição, disposto no artigo 12º da LPD, caracteriza-se como o poder pertencente ao titular dos dados de se opor ao tratamento dos mesmos, o que traduz a capacidade de cada indivíduo de controlar a utilização dos seus dados pessoais. O exercício deste direito pelo titular dos dados tem de se fundamentar em "razões ponderosas e legítimas" que justifiquem a sua oposição e que estejam relacionadas com a sua situação particular. A lei não enumera quais as "razões ponderosas e legítimas" que fundamentam o direito de oposição e, como tal, estas

terão de ser encontradas no caso concreto, balanceando os interesses do titular dos dados com os interesses do responsável pelo tratamento.

Existem, contudo, situações em que não faz sentido o direito de oposição ser invocado, nomeadamente, quando o tratamento dos dados tenha de se verificar para cumprir uma obrigação legal (artigo 6º, alínea b), ou quando tenha sido o próprio titular dos dados a consentir no tratamento (corpo do artigo 6º), bastando simplesmente revogar o seu consentimento.

Este direito revela-se importante nomeadamente nos casos de marketing (artigo 12º, alínea b), podendo neste caso, os titulares dos dados solicitar à Associação Portuguesa de Marketing Direto (APDM) que o seu nome integre a denominada "Lista Robinson", que contém o nome de todos os indivíduos que não pretendem ser incomodados por operações de marketing direto.

5.5. Confidencialidade no tratamento de dados

O artigo 17º da LPD consagra um dever de confidencialidade que se impõe não só ao responsável pelo tratamento como a todas as pessoas que inerentemente ao exercício das suas funções tenham contacto com dados pessoais. A violação do dever de sigilo conduz a responsabilidade criminal, segundo o disposto no artigo 47º da LPD e também segundo o artigo 195º (violação de segredo) e do artigo 384º (violação de segredo de correspondência ou de telecomunicações), ambos do Código Penal.

5.6. Condições de legitimidade para o tratamento de dados

Pelo facto de ser a lei a definir o conceito de dados pessoais, assim como as condições subjacentes ao seu tratamento, significa que não se encontra na disponibilidade de cada indivíduo proceder ao tratamento dos mesmos da maneira que entende, pois este está sujeito a condições de legalidade.

Consta da Lei de Proteção de Dados o regime a ser seguido no tratamento de dados pessoais e que de seguida analisaremos tendo em conta as suas especificidades.

5.6.1. Tratamento de dados sensíveis

As condições de legitimidade para o tratamento de dados pessoais sensíveis encontram-se no artigo 7º da LPD, considerando-se dados sensíveis, aqueles que respeitem a "(…) convicções filosóficas ou políticas, filiação partidária ou sindical, vida privada e origem racial ou étnica, bem como dados relativos à saúde e à vida sexual, incluindo os dados genéticos".

A Lei de Proteção de Dados consagra como princípio a proibição do tratamento de dados de natureza sensível. Os tratamentos de dados podem assumir um maior ou menor grau de sensibilidade, atendendo também ao contexto em que se enquadrem, uma vez que há dados que à partida não pertencem à categoria dos típicos dados sensíveis, mas podem revelar alguma sensibilidade num determinado contexto. Existem categorias de dados que, pelo seu caráter, são naturalmente considerados dados sensíveis, como os dados de saúde ou dados relativos à vida sexual.

O tratamento de dados sensíveis só poderá verificar-se se o responsável pelo tratamento obtiver o consentimento do titular dos mesmos ou se a lei autorizar esse tratamento. Na primeira situação - mediante consentimento do titular - o tratamento dos dados encontra-se dependente de autorização da CNPD que irá verificar se, no caso concreto, as condições de legitimidade do tratamento são cumpridas, isto é, se são adotadas medidas de segurança adequadas e se são respeitados os princípios de qualidade dos dados. Na segunda situação – em que o tratamento é permitido por uma disposição legal – a CNPD limitar-se-á a atribuir um parecer sobre essas disposições legais e o consequente tratamento de dados.

O tratamento de dados pessoais sensíveis, está sujeito a condições especiais, uma vez que este só pode realizar-se mediante a adoção de medidas especiais de segurança, tal como disposto no artigo 15º da LPD e também com garantias de não discriminação ao titular dos dados.

No âmbito dos dados sensíveis enquadra-se o conceito de vida privada que se tem revelado de difícil definição, uma vez que não é fácil delimitar as fronteiras da vida privada. Para a maioria da doutrina, o conceito de vida privada inclui as situações e os comportamentos dos indivíduos que não estão relacionados com a vida pública e que dizem respeito apenas à vida individual de cada um de nós. Na doutrina alemã foi desenvolvida uma teoria denominada de "Teoria das três esferas" e, segundo esta, podemos distinguir a vida íntima – situações que não são do conhecimento de mais ninguém a não ser do próprio indivíduo – a vida privada – engloba as situações que um indivíduo partilha mas apenas com um grupo restrito de pessoas – e a vida pública – que abrange as situações que podem ser do conhecimento de todos de modo geral.

Embora a Lei de Proteção de Dados portuguesa tenha transposto a Diretiva n.º 95/46/CE para o ordenamento jurídico português, não é daquela que surge a ideia de vida privada mas sim da Constituição.

5.6.2. Tratamento de dados relativos a suspeitas de atividades ilícitas, infrações penais e contraordenacionais

Estas categorias de dados pessoais estão autonomizadas no artigo 8º da LPD, logo, a lei não os qualifica como dados pessoais sensíveis. Todavia, os dados relativos a suspeitas de atividades ilícitas, infrações penais e contraordenacionais, bem como outras decisões que resultem na aplicação de uma pena, são dados que revestem características específicas e que, por isso, têm de ser autonomizados dos restantes. As condições de segurança inerentes ao tratamento deste tipo de informação terão de se revestir de alguma exigência.

5.6.3. Tratamento dos dados que não se incluem nas categorias acima descritas

Para que o tratamento de dados pessoais se afigure legítimo, tem de existir uma condição de legitimidade que o fundamente. Embora não possamos afirmar que os tratamentos de dados pessoais que não se enquadrem na categoria dos dados

sensíveis, por regra, são proibidos, serão permitidos apenas mediante condições que os legitimem. Por outras palavras, não podemos retirar do artigo 6º uma proibição genérica do tratamento de dados pessoais, mas sim duas limitações à concretização do tratamento: o consentimento do titular dos dados ou a necessidade do tratamento para as finalidades descritas nas alíneas do corpo do referido preceito.

O consentimento é a condição legitimante essencial, pelo facto de o tratamento de dados constituir uma intromissão na esfera do titular dos mesmos, estando aquele dependente de consentimento do titular. De modo geral, o consentimento traduz-se numa expressão de vontade livre, específica e informada, sendo que no caso de tratamento de dados sensíveis, o consentimento terá também de ser expressamente atribuído pelo titular dos dados. O consentimento não será valorado se a finalidade para a qual o mesmo foi recolhido não se encontrar perfeitamente delimitada.

Na situação prevista no artigo 6º, alínea a) - execução de contrato em que o titular seja parte ou diligências prévias à formação do mesmo - encontramos inúmeras situações que a ela se podem subsumir, como é o caso da aquisição de um bilhete, da contratação de serviços, da abertura de uma conta numa instituição bancária, entre outras situações. No caso da alínea b) - cumprimento de obrigação legal do responsável - por vezes existem situações em que é o próprio legislador que impõe a obrigatoriedade de um determinado tratamento, que é o que sucede, por exemplo, quando estipula a transmissão de dados de determinadas entidades para outras, como é o caso da comunicação de dados por parte do empregador à segurança social. Já na alínea c) o fundamento de legitimidade para o tratamento de dados pessoais consiste na necessidade de proteger interesses vitais do titular dos dados. Esta alínea abrange as situações em que o titular dos dados é incapaz (permanente ou temporariamente) assim como quando o titular dos dados é menor e não é possível obter consentimento do seu representante legal. A alínea d) - quando o tratamento de dados se afigurar necessário para a execução de uma missão de interesse público ou no exercício de autoridade pública - aplica-se aos casos em que um serviço público necessita de contactar um cidadão visando realizar um interesse público relevante. Por último, a alínea e) refere-se à prossecução de interesses legítimos do responsável ou de terceiro como condição de legitimidade do

tratamento de dados, desde que sobre aqueles não prevaleçam os interesses do titular dos dados.

5.7. Princípios da proteção de dados pessoais

5.7.1. Princípio da transparência

Este princípio implica que o responsável pelo tratamento dos dados deve dar a conhecer ao titular dos mesmos a finalidade inerente ao tratamento, as categorias de dados tratados, o seu período de conservação, as comunicações a que estejam sujeitos, entre outras informações relevantes no tratamento de dados. Expressão do princípio da transparência é o direito à informação e o direito de acesso, que visam que os tratamentos de dados pessoais sejam transparentes.

5.7.2. Princípio da finalidade ou da especificação da finalidade

Os dados recolhidos só podem ser utilizados no respeito pela finalidade que determinou a sua recolha, que deve encontrar-se determinada antes do início do tratamento, não podendo autorizar-se um tratamento de dados que não tenha uma finalidade determinada, explícita e legítima. Segundo o princípio da limitação do uso, os dados pessoais não podem ser tratados incompativelmente com a finalidade inicialmente definida. Contudo, existem situações em que é possível tratar os dados recolhidos no âmbito de uma finalidade distinta, carecendo esses tratamentos de controlo prévio por parte da CNPD (artigo 28º, n.º 1, alínea d), uma vez que é esta a autoridade competente para avaliar se a nova finalidade do tratamento é ou não compatível com a finalidade que determinou a recolha dos dados.

5.7.3. Princípios relativos à qualidade dos dados

A. Princípio da licitude e da lealdade

A licitude do tratamento afere-se tendo em conta o cumprimento das regras sobre proteção de dados. A lealdade está relacionada com o princípio da transparência, uma vez que os titulares dos dados têm o direito de saber quem é o responsável pelo tratamento, assim como a finalidade prosseguida pelo tratamento, verificando-se um tratamento desleal quando os titulares dos dados não possam opor-se à sua recolha.

B. Princípio da adequação, pertinência e proporcionalidade

Este princípio decorre do princípio da finalidade, na medida em que a adequação, pertinência e proporcionalidade dos dados recolhidos são determinados tendo em conta a finalidade do tratamento. A natureza dos dados pessoais objeto de tratamento tem de se afigurar idónea às finalidades prosseguidas pelo mesmo.

Por outro lado, o grau de utilização dos dados tem de ser o necessário para a prossecução da finalidade em concreto, uma vez que a recolha dos dados até pode ser adequada, mas se não for pertinente, então não se poderá autorizar o correspondente tratamento de dados. Por último, os dados tratados não podem ser excessivos relativamente à finalidade do tratamento, isto é, terá de se avaliar se o tratamento daquele dado em concreto é ou não necessário para a efetivação da finalidade.

C. Princípio da exatidão e atualização dos dados

A exatidão e a atualização dos dados têm igualmente de se verificar em comparação com a finalidade do tratamento. Dados desatualizados comportam consequências negativas não só para o titular dos dados, como para o responsável pelo tratamento, que vai estar a tratar dados que já não correspondem à realidade e

podem desfasar os resultados do tratamento. Já a exatidão dos dados pessoais, implica que o responsável pelo tratamento respeite o dever de retificação dos dados.

5.8. Videovigilância – análise dos casos suscitados no Gabinete de Atendimento ao Público

Tal como referi no ponto 4.8., analisarei a matéria relativa à videovigilância partindo de situações práticas que me foram colocadas, uma vez que é uma temática imensamente vasta e, além deste trabalho não se pautar apenas pela análise da videovigilância, também não temos espaço suficiente para lançar aqui uma discussão interessante sobre o tema.

A videovigilância consiste numa forma de vigilância à distância mediante a utilização de câmaras. O artigo 4º, n.º 4 da LPD estipula a aplicação desta lei aos tratamentos de dados operados através de câmaras de videovigilância. A utilização de sistemas de videovigilância vai diretamente ao encontro do direito à autodeterminação de cada indivíduo sobre a sua imagem e também do direito à reserva da intimidade da vida privada e do direito à autodeterminação informativa.

Existem casos em que a recolha de imagens não se configura necessariamente como um tratamento de dados pessoais, uma vez que não permitem a identificação dos indivíduos e, nesse caso, não se aplicará a Lei de Proteção de Dados. Por outras palavras, só estarão sujeitos à aplicação desta lei, a captação de imagens que permitam identificar pessoas. Por outro lado, para que aos tratamentos de imagens se apliquem as normas de proteção de dados, não tem de existir gravação das mesmas, uma vez que a simples captação se assume, só por si, como um tratamento de dados pessoais.

Igualmente importante de referir, é a não aplicação da Lei de Proteção de Dados à utilização de câmaras falsas. Uma vez que esta lei se aplica apenas quando existam tratamentos de dados pessoais, mediante a utilização de câmaras falsas não há lugar a qualquer captação de imagens e, como tal, não existe um tratamento de dados pessoais, logo, a utilização dessas câmaras não tem de respeitar nenhum preceito relativo à proteção de dados pessoais.

Do considerando 16 da Diretiva n.º 95/46/CE, retira-se que esta não terá aplicação aos tratamentos de som e imagem efetuados para fins de segurança pública. Todavia, esta exclusão não significa que no âmbito nacional seja proibida a utilização de imagens para esta finalidade.[109] Em Portugal, tem-se afigurado como fundamento à utilização da videovigilância para fins de segurança de pessoas e bens o Decreto-Lei n.º 35/2004, de 21 de fevereiro, que regula o exercício da segurança privada. A atividade de segurança privada assume uma função complementar à segurança pública do Estado.

5.8.1. Câmaras em ginásios que funcionam em horários noturnos[110]

Nesta situação, a questão colocada reportou-se a um ginásio que funciona em horários noturnos e os seus proprietários pretendiam instalar um sistema de videovigilância, colocando câmaras na entrada do mesmo e nos locais onde as pessoas estivessem a praticar a sua atividade física, com a finalidade de prevenir possível criminalidade associada ao funcionamento tardio das instalações.

Aliado aos princípios da qualidade dos dados estipulados na Lei de Proteção de Dados, o respeito pelo princípio da proporcionalidade assume-se fundamental no que se refere à legalidade de um tratamento de dados pessoais. Na utilização de sistemas de videovigilância, deve existir proporcionalidade na sua utilização, no sentido em que o recurso a este tipo de sistemas de tratamento de dados, deve ter em conta a finalidade da captação das imagens. No caso em concreto, a finalidade a ser prosseguida pela instalação deste sistema num ginásio assume-se legítima, uma vez que se destinava a assegurar a proteção de pessoas e bens.

O princípio da proporcionalidade também designado de princípio da proibição do excesso pretende assegurar o equilíbrio entre os direitos em causa numa determinada situação. Este princípio subdivide-se em três subprincípios: princípio da adequação, princípio da necessidade e princípio da proporcionalidade em sentido restrito. O princípio da adequação ou da conformidade dos meios estabelece que a

[109] Cf. artigo 4º, n.º 7 da LPD.

[110] Exemplos de instalação deste sistema em ginásios são as Autorizações n.º 1685/2006 e n.º 448/2009 emitidas pela CNPD disponíveis em http://www.cnpd.pt/bin/decisoes/aut/10_1685_2006.pdf ; http://www.cnpd.pt/bin/decisoes/aut/10_448_2009.pdf

prossecução de um dado interesse tem de estar numa relação de conformidade com o fim subjacente a esse interesse, ou seja, tem de existir uma relação de adequação entre a medida utilizada e o fim pretendido. Já o princípio da necessidade ou da exigibilidade pressupõe que o meio utilizado para atingir o fim terá de se afigurar o menos intrusivo e menos oneroso para os indivíduos. O terceiro subprincípio é o da proporcionalidade em sentido restrito. Por outras palavras, além de o fim a ser atingido ter de se demonstrar adequado e de não ter de existir outro meio igualmente eficaz e menos danoso em relação aos direitos fundamentais em causa, a medida terá também de se afigurar necessária e adequada para alcançar um determinado fim, tendo o resultado de se afigurar proporcional à restrição ocorrida. Em suma, o princípio da proporcionalidade opera em três vertentes: verifica a suscetibilidade da medida atingir o objetivo proposto, apurando a sua idoneidade nesse sentido, verifica a necessidade da medida por ser imprescindível para atingir o objetivo proposto de forma eficaz e, por último, pondera se da medida resultam mais vantagens ou prejuízos.

Assim, relativamente à videovigilância, o responsável pelo tratamento deve averiguar a sua adequação à finalidade pretendida, a indispensabilidade da sua utilização e a proporcionalidade dos sacrifícios que impõe aos utilizadores do ginásio. A videovigilância carateriza-se pelo seu caráter indispensável, sendo necessário recorrer a este mecanismo quando não exista uma alternativa menos intrusiva e menos restritiva da privacidade dos titulares dos dados para satisfazer os interesses do responsável pelo tratamento. Assim, a videovigilância configurar-se-á excessiva quando outros instrumentos menos onerosos e intrusivos para a privacidade dos titulares dos dados permitam atingir os mesmos objetivos e de forma eficiente.

Deste modo, na situação em apreço o direito à privacidade dos utilizadores do ginásio deve prevalecer sobre os interesses do proprietário do mesmo, uma vez que a adoção de um sistema de videovigilância não é imprescindível à manutenção da segurança do estabelecimento, pois a mesma poderá ser mantida optando por medidas menos intrusivas da privacidade dos seus utilizadores, uma vez que a existência de câmaras no espaço onde as pessoas estão a praticar as suas atividades traduz-se numa intromissão desproporcionada e excessiva às suas práticas.

5.8.2. Controlo do desempenho profissional de trabalhadores por meio de câmaras de videovigilância

O princípio da finalidade determina que as imagens não podem ser utilizadas para finalidades distintas das que determinaram a recolha dos dados pessoais. Segundo este princípio, as imagens recolhidas por um sistema de videovigilância instalado com a finalidade de proteção de pessoas e bens, não pode ser utilizado para efeitos de controlo dos trabalhadores.

A utilização de mecanismos de captação de imagens compromete a personalidade do trabalhador na relação de trabalho, na medida em que os trabalhadores não se sentem livres ao terem a perceção de que os dados recolhidos poderão ser utilizados para diversas finalidades. A instalação deste tipo de controlo por parte do empregador não pode ter por base apenas uma ideia de intromissão na vida privada do trabalhador.

É possível a instalação de sistemas de controlo e vigilância, tendo em conta o tipo de atividade em questão, desde que a sua utilização seja fundamentada, devendo ser sempre objeto de autorização por parte da CNPD.[111] Deve também ser acompanhada de um parecer prévio da Comissão de Trabalhadores como manifestação do princípio da transparência, na medida em que os representantes dos trabalhadores assumem um papel relevante no que se refere à garantia dos direitos fundamentais dos mesmos. Nesta medida, o parecer da Comissão de Trabalhadores complementa a autorização a ser atribuída pela CNPD, dotando-se, desta forma, o processo de algumas garantias, apesar de o papel primordial na aferição da legitimidade do tratamento caber à CNPD. O tratamento de dados pessoais será autorizado quando os princípios sejam respeitados e os instrumentos utilizados sejam necessários, adequados e proporcionais às finalidades pretendidas, ou seja, à proteção de pessoas e bens.

O consentimento do titular dos dados assume-se como um elemento essencial ao tratamento de dados pessoais, como estabelece o artigo 6º da LPD, ao se afirmar como uma condição de licitude da recolha dos dados. No entanto, no âmbito das

[111] Ver artigos 20º, n.º 2 e 21º, n.º 1 do Código do Trabalho

relações laborais é ambíguo falar-se de consentimento do titular dos dados, uma vez que este é o trabalhador que, por sua vez, se encontra numa relação de subordinação ao empregador e, como tal, não se poderá falar de um consentimento totalmente livre, de uma verdadeira liberdade de escolha, já que o trabalhador poderá consentir no tratamento dos seus dados com a finalidade de manter o seu posto de trabalho ou de conseguir o emprego.

Inerente ao contrato de trabalho naturalmente está a recolha de variadas informações do trabalhador para que o contrato de trabalho se torne exequível. Assim, no domínio das relações de trabalho, assume-se mais importante que o tratamento de dados retire a sua legitimidade do respeito pelo princípio da legitimidade e também pelo princípio da proporcionalidade, até porque o artigo 6º da LPD permite inúmeras exceções ao princípio da voluntariedade do tratamento de dados pessoais (consentimento do titular dos dados) permitindo logo na alínea a), a derrogação do consentimento do mesmo nas situações em que o tratamento dos dados seja necessário à execução de um contrato.

Só poderão ser instalados sistemas de videovigilância quando existam razões objetivas e justificadas para se restringirem direitos fundamentais dos trabalhadores, nomeadamente o seu direito à privacidade, uma vez que este tipo de controlo deverá ser adotado como *ultima ratio*, ou seja, quando mais nenhum outro meio se revelar eficaz para prosseguir as finalidades pretendidas pelo empregador. Igualmente fundamental para averiguar da licitude da utilização destes sistemas no local de trabalho é a ponderação de interesses, por um lado, do empregador, por outro lado, do trabalhador, tendo de existir um equilíbrio entre os mesmos, não podendo prevalecer os interesses de uma das partes sobre os interesses da outra, de forma completamente indiscriminada e aleatória. Deste modo, a adoção deste sistema de controlo dos trabalhadores, dependerá da existência ou não de um interesse jurídico relevante por parte do empregador.

Não se pode verificar um controlo constante por parte do empregador ao trabalhador, uma vez que o seu poder de controlo terá de se harmonizar com a liberdade, a dignidade e a privacidade dos trabalhadores, até porque uma vigilância constante dos trabalhadores gera um clima de desconforto e desconfiança nos mesmos. Neste sentido, o artigo 20º, n.º 1 do Código do Trabalho confere proteção

à privacidade do trabalhador no seu local de trabalho, embora não tutele de forma absoluta a privacidade do mesmo, ao permitir a utilização destes sistemas mediante determinadas condições no seu n.º 2.

Assim, a ideia a reter é a de que a instalação de câmaras de videovigilância que se destinem a controlar a atividade dos trabalhadores e que tenham nessa finalidade o seu único objetivo, não é lícita e, por isso, proibida, independentemente de o trabalhador conhecer da sua existência, pois esse facto não atribui licitude ao atentado contra a sua dignidade e privacidade. Controlar o desempenho profissional do trabalhador não se considera uma finalidade legítima na aceção do artigo 5º da LPD, por não se configurar uma medida necessária à execução do contrato de trabalho e porque limita a liberdade do trabalhador, anulando a sua esfera de privacidade no local de trabalho, existindo, portanto, um desvio ao princípio da finalidade, pilar fundamental na licitude do tratamento de dados pessoais.

Só em circunstâncias excecionais pode o empregador submeter o trabalhador a um controlo, nomeadamente, quando este seja indispensável por motivos de segurança de pessoas e bens ou por razões relacionadas com a natureza da atividade em causa, ao ponto de a não existência de controlo se traduzir em consequências mais gravosas para a empresa, do que as consequências do controlo se traduzem para os trabalhadores. Só poderão instalar-se estes sistemas por motivos de segurança de pessoas e bens quando, além de existir um perigo real à manutenção dessa segurança, aquele auxilie na prevenção da prática de infrações graves. Logo, a adoção destes sistemas não será admissível quando visem prevenir pequenas infrações ou para desincentivar pequenos furtos.

Essencial à instalação deste tipo de sistemas no local de trabalho é o princípio da intromissão mínima, que se traduz na necessidade de o empregador limitar os direitos fundamentais do trabalhador no mínimo possível, adotando as medidas menos lesivas e estritamente necessárias à finalidade prosseguida, com o intuito de minimizar os efeitos para a privacidade dos trabalhadores. Este princípio impõe que o empregador seja minucioso na instalação do sistema de videovigilância, nomeadamente, no ângulo de captação das imagens, o espaço que as mesmas irão captar, a suficiência da mera visualização das imagens em vez de captar e gravar as mesmas, a localização das câmaras, não podendo o empregador instalar câmaras em

locais reservados aos trabalhadores, como os vestiários, salas de descanso, entre outros locais onde não sejam executados trabalhos e onde os trabalhadores manifestam a sua privacidade.

5.8.3. Utilização como meio de prova de imagens captadas por sistemas de videovigilância não legalizados

Uma das questões suscitadas no domínio da videovigilância prende-se com o facto de um determinado estabelecimento ter instalado um sistema de videovigilância sem possuir autorização da CNPD para o efeito. Ocorrendo a prática de um ato ilícito, que fica registado nas imagens captadas pelas câmaras, o proprietário do estabelecimento pretende utilizar essas imagens como meio de prova. Questão pertinentemente colocada relaciona-se com a possibilidade de essas imagens serem utilizadas como meio de prova, uma vez que foram captadas por sistemas de videovigilância não legalizados.

O desrespeito pelo dever de notificação da instalação do sistema à CNPD não tem como consequência única a aplicação de uma coima. A falta de notificação de um tratamento de dados pessoais por meio de videovigilância, implica que as imagens captadas que comprovem a prática de um ato ilícito não possam ser utilizadas como meio de prova. Ou será que podem?

O artigo 125º do Código de Processo Penal (CPP) estipula o princípio da legalidade da prova, nos termos do qual "são admissíveis as provas que não forem proibidas por lei". Ao proibir a utilização de determinados meios de prova, esta norma determina, numa interpretação a contrário, que são admissíveis como meios de prova todos aqueles que o direito não proíbe. Nas palavras de GERMANO MARQUES DA SILVA existe uma "liberdade da prova" [112] o que significa que são admitidos meios de prova atípicos (meios de prova que não se encontram estabelecidos na lei).

[112] GERMANO MARQUES DA SILVA - *Curso de Processo Penal*, Volume II, 5ª Edição, p. 167.

Segundo o artigo 126º do CPP[113], são proibidas as provas obtidas mediante violação da integridade física e moral das pessoas, assim como as provas obtidas através do desrespeito pela sua privacidade. As proibições de prova relacionam-se com o modo ilícito como os meios de prova foram obtidos[114] originando provas nulas.[115] O referido preceito estabelece métodos de prova cujo uso é inadmissível, por corresponderem a violações intoleráveis à dignidade humana e a direitos fundamentais e que, por isso, não podem ser valorados pelo julgador no processo.

Quanto ao regime da nulidade da prova proibida, quando a prova proibida atinja o direito à integridade física e moral, a sua nulidade é insanável (126º, n.º 1 e 2), enquanto a prova proibida que atinge o direito à privacidade (126º, n.º3) inclui-se num regime de nulidade sanável mediante o consentimento do titular do direito. Assim, as provas obtidas por intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, são consideradas provas relativamente proibidas, pelo facto de puderem ser utilizadas não só quando o titular dos direitos violados anuir na sua utilização, mas também nas situações descritas nos números 2, 3 e 4 do artigo 34º da CRP. Esta nulidade relativa só pode ser conhecida por

---

113

Artigo 126.º

Métodos proibidos de prova

1 — São nulas, não podendo ser utilizadas, as provas obtidas mediante tortura, coação ou, em geral, ofensa da integridade física ou moral das pessoas.

2 — São ofensivas da integridade física ou moral das pessoas as provas obtidas, mesmo que com consentimento delas, mediante:

a) Perturbação da liberdade de vontade ou de decisão através de maus tratos, ofensas corporais, administração de meios de qualquer natureza, hipnose ou utilização de meios cruéis ou enganosos;
b) Perturbação, por qualquer meio, da capacidade de memória ou de avaliação;
c) Utilização da força, fora dos casos e dos limites permitidos pela lei;
d) Ameaça com medida legalmente inadmissível e, bem assim, com denegação ou condicionamento da obtenção de benefício legalmente previsto;
e) Promessa de vantagem legalmente inadmissível.

3 — Ressalvados os casos previstos na lei, são igualmente nulas, não podendo ser utilizadas, as provas obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações sem o consentimento do respetivo titular.

4 — Se o uso dos métodos de obtenção de provas previstos neste artigo constituir crime, podem aquelas ser utilizadas com o fim exclusivo de proceder contra os agentes do mesmo.

114 Cf. artigo 167º CPP.

115 Artigo 32º, n.º 8 CRP.

requerimento do titular do direito infringido, não podendo o juiz conhecê-la oficiosamente.

Segundo FREDERICO DA COSTA PINTO[116], "no direito processual penal todas as provas proibidas são ilegais mas nem todas as provas ilegais são provas proibidas". Serão meios de prova admissíveis os que não se assumirem ilícitos para o direito penal. São penalmente ilícitos quando realizarem os tipos incriminadores dos artigos 192º e 199º do Código Penal. [117]

O legislador penal ao estabelecer a proibição de valoração de prova obtida de forma ilícita pode colocar em risco a descoberta da verdade, já que essa prova pode afigurar-se crucial na reconstituição do facto e, ao não ser utilizada, o processo pode ter um desfecho diferente daquele que teria se a prova pudesse ser utilizada. Todavia, pretendeu o legislador que a verdade dos factos não fosse encontrada a todo o custo, inclusive colocando em causa direitos fundamentais dos indivíduos. A proibição de meios de prova que atentem contra direitos fundamentais das pessoas constitui uma garantia do processo criminal, disposta no artigo 32º, n.º 8 da CRP.

Impõe-se retirar as ideias fundamentais estabelecidas nos preceitos aqui envolvidos. O artigo 167º do CPP refere que as reproduções fotográficas ou obtidas por instrumentos eletrónicos só valem como prova a ser valorada no processo criminal, quando obtidas de forma lícita. No mesmo sentido, o artigo 126º, n.º 3 estabelece uma proibição relativa de utilização de provas que tenham sido obtidas mediante intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações, desde que o titular desses direitos não tenha expresso o seu consentimento para essa utilização.

Já no Código Penal, o artigo 192º incrimina as atuações que devassem a vida privada de outra pessoa, nomeadamente, no que aqui nos interessa, através da captação e registo da imagem de outra pessoa (alínea b) do n.º 1). Interpretando o n.º 2 do preceito a *contrario sensu*, podemos concluir que os factos descritos nas alíneas a), b) e c) do n.º 1 serão sempre punidos, mesmo que o agente atue em defesa de um interesse público legítimo e relevante, não se justificando em alguma

[116] FREDERICO DE LACERDA DA COSTA PINTO – "Depoimento Indireto, Legalidade da prova e direito de defesa", in *Estudos em Homenagem ao Professor Doutor Jorge de Figueiredo Dias*, Volume III, p. 1071.

[117] O artigo 192º contempla o crime de devassa da vida privada, enquanto o artigo 199º se refere ao crime de gravações e fotografias ilícitas.

circunstância a devassa na vida privada de outra pessoa. Já o artigo 199º refere-se a gravações e fotografias ilícitas que estabelece a punição para quem "fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado".

Por sua vez, a Constituição estabelece a nulidade de todas[118] as provas obtidas através de abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações[119].

Analisando a legislação referida, podemos afirmar que as imagens captadas por sistemas de videovigilância não autorizados previamente ao acontecimento dos factos criminosos, não podem ser utilizadas como meios de prova em processo penal, por estarem a recolher imagens de forma ilícita. Porém, apesar de este entendimento parecer o único a ser acolhido, existem divergências na jurisprudência ao existirem diferentes perspetivas e abordagens por parte dos julgadores nos tribunais portugueses.

No acórdão de 26/03/2008, o Tribunal da Relação do Porto[120] entendeu que "podemos concluir que os fotogramas obtidos através do sistema de videovigilância existentes num centro de lavagem, para proteção dos seus bens e da integridade física de quem aí se encontre, mesmo que se desconheça se esse sistema foi comunicado à CNPD, não correspondem a qualquer método proibitivo de prova, desde que exista uma justa causa para a sua obtenção, como é o caso de documentarem a prática de uma infração criminal, e não digam respeito ao "núcleo duro da vida privada" da pessoa visionada".

Também emanado pelo Tribunal da Relação do Porto, o acórdão de 23/10/2013[121] refere que "São válidas, podendo ser valoradas pelo julgador (não constituindo métodos proibidos de prova) as provas que consistem na gravação de imagens feita por particular (ofendido). A gravação de imagens em local público, por

[118] Sublinhado meu.

[119] Cf. artigo 32º, n.º 8.

[120] Acórdão disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/24cd01e84ff51ff88025741e0034cc7e?OpenDocument&Highlight=0,imagens,como,meio,de,prova (consultado a 4 julho 2014).

[121] Acórdão disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/301ec6a6cdd8ceab80257c1a005a61e4?OpenDocument&Highlight=0,imagens,como,meio,de,prova (consultado a 4 julho 2014).

factos ocorridos na via pública, sem conhecimento do visionado, tendo como única finalidade a identificação do autor do crime de dano (que atinge o património do particular que fez a filmagem), mesmo que não haja prévio licenciamento pela Comissão Nacional de Protecção de Dados, constitui prova por neste caso existir justa causa para essa captação de imagens (desde logo documentar a prática de infração criminal que atenta contra o património do autor da filmagem). A imagem captada nas circunstâncias deste caso concreto, por um lado não constitui nenhuma violação do "núcleo duro da vida privada", nem do direito à imagem do visionado, não sendo necessário o seu consentimento para essa gravação, tal como decorre do art. 79º, nº 2, do CC (estando a filmagem do suspeito justificada por exigências de justiça) e, por outro lado, aquela conduta do particular que fez a filmagem de imagens em local público não constitui a prática do crime de "gravações e fotografias ilícitas" p. e p. no art. 199º, nº 2, do CP, nem tão pouco integra a prática de qualquer ilícito culposo segundo o ordenamento jurídico, mesmo considerado este globalmente".

O acórdão do Tribunal da Relação de Évora datado de 24/04/2012 [122], afirma mesmo que "A questão da validade da prova assente na obtenção e utilização da recolha de imagens não depende de que esta esteja, ou não, autorizada pela Comissão Nacional de Protecção de Dados".

Entendimento contrário perfilha o acórdão do Tribunal da Relação de Lisboa[123]de 30/10/2008, no qual podemos ler "É pacífico que a licitude da videovigilância se afere pela sua conformidade ao fim que a autorizou. O fim visado pela videovigilância instalada na escola, um local público, por um cidadão, só poderia ser exclusivamente o de prevenir a segurança do estabelecimento, mas devendo conter o aviso aos que lá se encontram ou se deslocam de que estão a ser filmados e só, nesta medida, a videovigilância é legítima. Não basta que as referidas imagens tenham sido colhidas numa escola pública, em local público e de não visarem o contexto da vida privada dos arguidos, enquanto

[122]Acórdão disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/c7875c514b7fa32a802579ff003e21b7?OpenDocument&Highlight=0,imagens,como,meio,de,prova (consultado a 4 julho 2014).

[123]Acórdão disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c222f7dd896e84da802575010043b3dc?OpenDocument&Highlight=0,videovigil%C3%A2ncia,como,meio,de,prova (consultado a 4 julho 2014).

autores do crime de furto qualificado, para se concluir, que a utilização dessas imagens não viola a intimidade ou a esfera privada dos arguidos. Na verdade, as imagens oferecidas como meio de prova não obedeceram aos requisitos impostos por lei, ou seja, o cidadão não estava autorizado para o fazer e o sistema de videovigilância não se encontrava devidamente assinalado, sendo que, nestas circunstâncias as imagens constituem, uma abusiva intromissão na vida privada e a violação do direito à imagem dos arguidos."

Constatamos, assim, que não existe um entendimento comum na jurisprudência portuguesa relativamente à utilização de imagens captadas por sistemas de videovigilância não legalizados como prova em processo penal. Quem entende que as imagens captadas por sistemas de videovigilância não podem ser utilizadas em processo penal, por serem métodos proibitivos de prova, defende a sua posição utilizando argumentos que vão ao encontro dos referidos preceitos do Código Penal, do Código de Processo Penal e da Constituição Portuguesa. Por sua vez, quem assume a valoração dessas imagens como meio de prova fundamenta que as mesmas não incidem sobre a intimidade da vida privada do agente do crime pelo facto de as câmaras se encontrarem em locais públicos e também por existir uma justa causa para a utilização das mesmas, estabelecida no artigo 79º, n.º 2 do Código Civil, mais precisamente, por se configurar uma exigência de justiça ou de polícia.

Em meu entender, não faz sentido que o direito à imagem e o direito à privacidade do agente que pratica um ato ilícito prevaleça de tal modo que o agente seja protegido pelo sistema jurídico, impedindo a sua punição pela prática de um ato criminoso, independentemente de o sistema de videovigilância estar legalizado ou não junto da CNPD. O Supremo Tribunal de Justiça afirma que a proteção da imagem que retrata uma prática criminosa tem de ceder, uma vez que " (…) a proteção acaba quando aquilo que se pretende proteger constitui um crime". [124] Por esta razão, defendo que deverá existir uma dupla responsabilização, isto é, o agente que praticou o ato ilícito deverá ser punido pelo tipo incriminador que a sua conduta preencheu, aceitando-se como prova da prática do ato as imagens captadas por videovigilância, assim como o responsável pelo tratamento deverá responder

[124] Acórdão do Supremo Tribunal de Justiça de 29-09-2011, no âmbito do processo 22/09.6YGLSB.S2

pela não legalização do sistema que instalou, nos termos da Lei de Proteção de Dados.

Pode-se, no entanto, estabelecer limites à utilização dessas imagens num processo criminal, atendendo à gravidade da infração praticada. Se estivermos perante a prática de um ilícito de "pouca gravidade", por exemplo, o agente furtou de uma ourivesaria uma pulseira no valor de 200 euros, a utilização das imagens ilegalmente obtidas não devem ser utilizadas. Se, por outro lado, o agente praticou um homicídio, as imagens deverão ser utilizadas como meio de prova. No entanto, uma solução que assente na gravidade da infração praticada pode não resultar na prática, uma vez que no caso do roubo da pulseira, 200 euros pode considerar-se um valor diminuto para uma ourivesaria, mas assim já não é se a pulseira tiver sido furtada de uma pessoa.

Uma outra solução, possivelmente mais equilibrada que a primeira, é utilizar como critério a exclusividade do meio de prova, isto é, admitir a utilização das imagens como meio de prova quando não exista nenhum outro meio a que se possa recorrer para provar a prática do crime, afigurando-se, portanto, essas imagens como meio de prova único.

5.8.4. Controlo oculto por meio de videovigilância

Igualmente colocada foi a questão de saber se existia mesmo necessidade de avisar a existência de um sistema de videovigilância em funcionamento e quais eram as caraterísticas obrigatórias desses avisos informativos. Tendo em conta o princípio da transparência do tratamento de dados pessoais e o direito de informação aos titulares dos dados, seja no âmbito laboral ou fora dele, não poderá existir um controlo oculto sobre os titulares dos dados, independentemente do meio de controlo utilizado. Esta proibição decorre do princípio da boa-fé, do direito à privacidade e da dignidade da pessoa humana, uma vez que caso fossem permitidos tratamentos de dados pessoais sem que os titulares desse facto tivessem conhecimento, existiriam violações claras aos direitos fundamentais dos cidadãos.

Todavia, coloca-se a questão de saber se em determinadas circunstâncias será possível recorrer a meios visuais de controlo sem que o titular dos dados tenha

conhecimento da sua existência. De facto, recorrer a um controlo oculto pode ser útil para desvendar a prática de atividades ilícitas, nomeadamente no âmbito de um contrato de trabalho, quando necessário para desvendar a responsabilidade de certos atos. Contudo, embora em situações de *ultima ratio* este tipo de controlo se pudesse afigurar útil, não nos parece que os princípios basilares do tratamento de dados pessoais fossem respeitados ao ser permitida tal atuação, não se devendo permitir derrogações aos mesmos, uma vez que visam proteger direitos constitucionalmente consagrados.

No âmbito laboral o artigo 20º do Código do Trabalho afasta a possibilidade da existência de um controlo desse género. O mesmo sucede no controlo de áreas públicas, sendo obrigatória a existência de um aviso informativo sobre a existência de um dispositivo eletrónico de controlo.

A questão do controlo oculto parece identificar-se com a questão da utilização de imagens para fins de prova em processo penal, uma vez que no primeiro caso estamos perante situações em que se pretende efetuar um controlo propositado com a finalidade de se descobrir a identidade do autor de atos ilícitos e, no segundo caso, o sistema foi instalado sem para tal ter autorização e no decorrer da sua utilização ocorreu um ato criminoso e, em consequência, pretende-se utilizar essas imagens para provar o sucedido. Digo que estas questões parecem identificar-se e não que se identificam, uma vez que o cerne das mesmas não é igual. Enquanto a finalidade da realização de um controlo oculto se prende exatamente com o ato de controlar determinada pessoa ou determinado local para "apanhar" quem pratique atos ilícitos, sem que os sujeitos visionados se apercebam da existência do sistema, na utilização de imagens para meios de prova o que sucede é que no decorrer do funcionamento de um sistema ilegal ocorreu a prática de um crime. Trata-se, portanto, da finalidade visada, não sendo permitido o funcionamento de sistemas que visem controlar pessoas, uma vez que a videovigilância encontra o seu escopo na proteção de pessoas e bens e não no controlo de pessoas e bens.

Relativamente às caraterísticas do aviso informativo da existência de um sistema de videovigilância, estas encontram-se estabelecidas no artigo 31º, n.º 5 da

Lei n.º 34/2013, de 16 de maio[125] e também no artigo 115º da Portaria n.º 273/2013, de 20 de agosto.[126]

5.9. Consequências do desrespeito pelas normas de proteção de dados

A Lei de Proteção de Dados prevê instrumentos que visam assegurar o cumprimento das normas de proteção de dados, tanto por via administrativa, como por via jurisdicional. No que se refere às sanções administrativas, a LPD estabelece as situações que constituem contraordenação nos artigos 37º e 38º. Destes preceitos constam as situações em que o responsável pelo tratamento não cumpriu ou cumpriu de forma incompleta as suas obrigações no tratamento de dados pessoais.

As atuações negligentes por parte dos responsáveis pelo tratamento, assim como as tentativas, são puníveis nos termos do artigo 40º da LPD.

---

[125] Disponível em http://www.cnpd.pt/bin/legis/nacional/Lei_34_2013_Seguranca_privada.pdf (consultado a 4 julho 2014).
"Nos locais objeto de vigilância com recurso a câmaras de vídeo é obrigatória a afixação, em local bem visível, de informação sobre as seguintes matérias:

a) A existência e localização das câmaras de vídeo;
b) A menção «Para sua proteção, este local é objeto de videovigilância»;
c) A entidade de segurança privada autorizada a operar o sistema, pela menção do nome e alvará ou licença;
d) O responsável pelo tratamento dos dados recolhidos perante quem os direitos de acesso e retificação podem ser exercidos."

[126] Disponível em http://dre.pt/pdf1sdip/2013/08/15900/0495604988.pdf (consultado a 4 julho 2014).
"1 — O símbolo identificativo a utilizar na identificação dos locais objeto de vigilância com recurso aos meios previstos no n.°1 do artigo 31.° da Lei n.°34/2013, de 16 de maio, constam do anexo VIII à presente portaria, da qual faz parte integrante.

2 — Os requisitos e especificações técnicas da sinalização e as suas dimensões devem cumprir as disposições da norma ISO 3864-1.

3 — O aviso a que se refere o n.°5 do artigo 31.° da Lei n.°34/2013, de 16 de maio, deve ser colocado de forma a garantir boas condições de legibilidade das mensagens nele contidas e a acautelar a normal circulação e segurança dos utentes dos espaços.

4 — Os avisos são colocados no perímetro exterior do local ou zona objeto de vigilância com recurso a equipamentos eletrónicos de videovigilância por câmaras de vídeo, e da forma mais conveniente ao seu pronto reconhecimento pelos utentes.

5 — No interior do local ou zona objeto de vigilância devem ser repetidos os avisos de informação."

No ANEXO VIII consta a forma de sinalização do sistema de videovigilância em funcionamento: **"**Sinal em forma de triângulo equilátero, em fundo de cor amarela com orla interior em cor preta, ao centro, símbolo representando o pictograma de uma câmara de videovigilância em cor preta".

No que se refere aos crimes, contempla a LPD, que conduz à prática de um crime o não cumprimento de obrigações referentes à proteção de dados, o acesso indevido a dados pessoais, a viciação ou destruição dos mesmos, a desobediência qualificada às notificações da CNPD para cessar ou bloquear um tratamento de dados e também a violação do dever de sigilo, crimes dispostos nos artigos 43º a 47º. No caso de prática de crimes, a ação penal terá de ser prosseguida pelo Ministério Público, competindo à CNPD participar de todas as situações de que tenha conhecimento.

Quando estejamos perante um concurso de infrações, isto é, se o mesmo facto constituir simultaneamente crime e contraordenação, prevalecerá o crime, sendo o agente punido pela prática do mesmo. Por outro lado, se ao mesmo agente for imputada a prática de mais do que uma contraordenação, estas serão cumuladas, conforme resulta do artigo 39º da LPD.

Igualmente importante é o direito de audiência prévia, estipulado no artigo 50º do Regime Geral das Contraordenações, que deverá ser respeitado pela CNPD no momento da aplicação das coimas ao agente, caso contrário, a sua decisão de aplicação das mesmas não será válida, por violar o disposto no artigo 32º, n.º 10 da Constituição da República Portuguesa.

Quando a contraordenação resultar da omissão de um dever, o infrator deverá cumprir a obrigação a que estava sujeito, independentemente do pagamento da coima por incumprimento dessa obrigação, ou seja, se a contraordenação resultar da omissão de um dever, o agente estará obrigado ao seu cumprimento, nos casos em que seja possível cumpri-lo.

Conjuntamente à imputação do crime ou da contraordenação ao agente, a LPD prevê ainda a aplicação de sanções acessórias no artigo 49º. Outra consequência do incumprimento de disposições de proteção de dados, consiste na advertência da Comissão ao agente. Estabelece ainda a LPD um princípio de responsabilidade civil no artigo 34º, segundo o qual todos aqueles que tenham sofrido prejuízos derivados de um tratamento ilícito de dados pessoais, têm o direito a ver esses danos ressarcidos. Por outro lado, podem ainda ser utilizadas providências preventivas designadas no direito civil (cf. artigo 70º, n.º 2 do Código Civil).

As decisões da CNPD podem ser judicialmente impugnadas para o Tribunal da Concorrência, Regulação e Supervisão de Santarém, por se afigurar o tribunal de competência especializada para conhecer das questões relativas a processos de contraordenação de entidades administrativas independentes, como é o caso da Comissão.

6. Conclusão

No decorrer da elaboração do presente relatório foram várias as reflexões que surgiram, o que demonstra que a proteção de dados pessoais não é um assunto que esteja resolvido e que tenha respostas certas e inequívocas. Pelo contrário, é um tema cada vez mais atual, constantemente desafiado na sociedade em que vivemos e que, por isso, merece toda a atenção e reflexão, de modo a permitir que vivamos num mundo equilibrado e que respeite os direitos fundamentais inerentes à condição humana.

Tanto no âmbito europeu como além dele, é inúmera a legislação que pretende delinear a proteção dos dados pessoais e da vida privada dos cidadãos, atribuindo-lhe a natureza de direito fundamental, como é o caso da Carta dos Direitos Fundamentais da União Europeia, das Diretivas Comunitárias, da Constituição da República Portuguesa, assim como variada legislação estabelecida em diplomas avulsos. Alguns destes diplomas avulsos têm aplicação a setores muito específicos, tendo em conta os domínios que se pretendem abranger com a aplicação de determinadas normas. Neste sentido, o Conselho da Europa produz diversas Recomendações com o intuito de criar regulamentação mais pormenorizada, dirigida a certos setores de atividade.

Na sociedade da informação atual, assiste-se a um conflito permanente entre dois grandes valores: a segurança, que tem vindo a ganhar cada vez maior relevo e a privacidade inerente a cada cidadão. A segurança é essencial na vida de todos nós, pois existindo um clima de paz e de confiança, sentiremos liberdade para exercer os nossos direitos. O direito à segurança é, portanto, uma garantia do exercício de outros direitos. O Tribunal Europeu dos Direitos do Homem reconhece que os interesses de segurança nacional prevalecem sobre os interesses individuais, embora não os devam ultrapassar. Impõe-se discernir até que ponto a necessidade de

segurança pode limitar os nossos direitos individuais. Esta ideia tem aplicação aos tratamentos de dados pessoais que impliquem vigilância, sob qualquer forma, dos titulares dos dados, tomando como exemplo a luta contra o terrorismo desencadeada após os acontecimentos de 11 de setembro de 2001 que têm fundamentado a adoção de políticas securitárias, alterando o equilíbrio que vigorava no binómio liberdade/segurança. A necessidade de lutar mais eficazmente contra o terrorismo impõe a adoção de medidas suscetíveis de pôr em perigo as liberdades fundamentais, nomeadamente a privacidade.

Em Portugal, é a Constituição o instrumento adequado para balancear o conflito entre liberdade particular e interesse público.

Os tratamentos de dados a realizar, bem como os meios utilizados devem apresentar-se necessários, adequados e proporcionais às finalidades estabelecidas para os mesmos. Para se concluir pela proporcionalidade de uma medida restritiva de um direito fundamental importa acolher o seguinte raciocínio: a medida adotada é idónea para alcançar o objetivo proposto (princípio da idoneidade), necessária, tendo a capacidade de atingir o objetivo com a eficácia que mais nenhuma medida conseguirá (princípio da necessidade) e também se a medida é equilibrada de modo que atinja benefícios superiores quando confrontados com outros bens ou valores (proporcionalidade em sentido restrito). O princípio da proporcionalidade implica, portanto, um juízo de idoneidade do meio utilizado, assim como a verificação do princípio da intervenção mínima, estando necessariamente inerente uma ponderação entre a finalidade prosseguida pelo tratamento de dados e os direitos fundamentais suscetíveis de serem violados.

Com o surgimento da sociedade da informação, para trás ficaram os tempos em que a cedência de dados pessoais por parte dos seus titulares era contida. Na atualidade, a maioria dos cidadãos acha normal ceder os seus dados sem sequer questionar para que finalidade os mesmos serão usados, muitas das vezes desconhecendo quem é o responsável pela recolha, encarando com absoluta normalidade situações em que deveria adotar uma atitude cautelosa. O que porventura nos esquecemos é que a perda da nossa privacidade pode significar a perda da nossa segurança.

A internet continuará a liderar os desafios que se impõem à proteção de dados pessoais, uma vez que comporta inúmeros riscos e perigos para os seus utilizadores, não só pelo facto de ser global, o que permite que uma pessoa em qualquer parte do mundo possa saber tudo sobre outra que se encontra a milhares de quilómetros, como também pela quantidade de informação que é "despejada" no mundo virtual, o que leva a uma elevada concentração de informação sobre cada utilizador, existindo uma excessiva aglomeração de dados, o que se pode tornar verdadeiramente perigoso, já que é suficiente que alguém mal intencionado se dê ao trabalho de acumular informações sobre determinada pessoa, para a sua vida se tornar num autêntico "Big Brother".

A verdade é que a par dos seus perigos, a internet é uma tecnologia verdadeiramente revolucionária, pois a partir dela temos ao nosso dispor instrumentos fantásticos de lazer, de trabalho, de negócios, já que podemos fazer praticamente de tudo através da internet, sem termos de sair do sítio e de forma muito mais facilitada.

O ritmo da evolução tecnológica não vai abrandar, surgindo todos os dias novos desafios para a proteção dos dados pessoais e para a privacidade dos cidadãos, competindo às instâncias nacionais e europeias antecipar os avanços tecnológicos, não deixando margem para uma total desproteção dos direitos fundamentais dos cidadãos.

Página propositadamente deixada em branco

Bibliografia

Monografias

ALBUQUERQUE, PAULO PINTO SÉRGIO DE

- *Comentário do Código Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 2ª edição, Lisboa, Universidade Católica Editora, 2010, 1327 p. ISBN 978-972-54-0272-6.

- *Comentário do Código de Processo Penal: à luz da Constituição da República e da Convenção Europeia dos Direitos do Homem*, 4ª edição, Lisboa, Universidade Católica Editora, 2011, 1712 p. ISBN 978-972-54-0295-5.

BELLEIL, ARNAUD – *Privacidade – o mercado dos dados pessoais: proteção da vida privada na idade da internet*, Lisboa, Instituto Piaget, 2001, 210 p. ISBN 972-771-597-4.

CANOTILHO, JOSÉ JOAQUIM GOMES; MOREIRA, VITAL – *Constituição da República Portuguesa Anotada*, Vol. I, 4ª edição (revista), Coimbra, Coimbra Editora, 2007, 1085 p. ISBN 978-972-32-1462-8.

CASTRO, CATARINA SARMENTO E – *Direito da Informática, privacidade e dados pessoais*, Coimbra, Edições Almedina, 2005, 374 p. ISBN 972-40-2424-5.

COSTA, MÁRIO JÚLIO DE ALMEIDA – *Direito das Obrigações*, 12ª edição (revista e atualizada), Coimbra, Edições Almedina, 2009, 1146 p. ISBN 978-972-40-4033-2.

FARINHO, DOMINGO SOARES – *Intimidade da vida privada e media no ciberespaço*, Coimbra, Edições Almedina, 2006, 104 p. ISBN 972-40-2740-6.

GOMES, MÁRIO MANUEL VARGES – *O Código da privacidade e da proteção de dados pessoais: na lei e na jurisprudência*, Lisboa, Centro Atlântico, 2006, 568 p. ISBN 989-615-022-2.

GUERRA, AMADEU

– "A Lei de Proteção de Dados Pessoais", Associação Portuguesa do Direito Intelectual in *Direito da sociedade da informação*, Vol. II, Coimbra, Coimbra Editora, 2001, ISBN 972-32-0994-2, p. 145-170.

- "A utilização de sistemas de vídeo pelas forças e serviços de segurança em locais públicos – Reflexões sobre a Lei n.º 1/2005, de 10 de janeiro", in *Revista do Ministério Público*, N.º 103, Lisboa, Editorial Minerva, Ano 26, Julho-Setembro 2005, ISSN 0870-6107, p. 39-63.

LEITÃO, LUÍS MANUEL TELES DE MENEZES – *Cessão de Créditos*, Coimbra, Edições Almedina, 2005, 669 p. ISBN 972-40-2505-5.

MARQUES, GARCIA; MARTINS, LOURENÇO – *Direito da Informática*, 2ª edição (reformulada e atualizada), Coimbra, Coimbra Editora, 2006, 575 p. ISBN 972-40-2859-3.

MONTEIRO, ANTÓNIO PINTO – *As telecomunicações e o direito na sociedade da informação: Atas do colóquio organizado pelo IJC em 23 e 24 de abril de 1998*, Coimbra, Instituto Jurídico da Comunicação, 1999, 390 p. ISBN 972-98462-0-0.

MOREIRA, TERESA ALEXANDRA COELHO – *A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação: contributo para um estudo dos limites do poder de controlo eletrónico do empregador*, Coimbra, Edições Almedina, 2010, 893 p. ISBN 978-972-40-4208-4. Tese de doutoramento.

PINTO, CARLOS ALBERTO DA MOTA; MONTEIRO, ANTÓNIO PINTO; PINTO, PAULO MOTA – *Teoria Geral do Direito Civil*, 4ª edição (2ª reimpressão), Coimbra, Coimbra Editora, 2012, 687 p. ISBN 978-972-32-2102-2.

PINTO, FREDERICO DE LACERDA DA COSTA – "Depoimento Indireto, Legalidade da Prova e Direito de Defesa", Boletim da Faculdade de Direito da Universidade de Coimbra, in *Estudos em Homenagem ao Professor Doutor Jorge de Figueiredo Dias*, Vol. II, Coimbra, Coimbra Editora, 2010, p. 1041-1088.

SILVA, GERMANO MARQUES DA – *Curso de Processo Penal*, Vol. II, 5ª edição, Lisboa, Verbo, 2011, 464 p. ISBN 978-972-22-3043-8.

Documentos disponíveis em formato eletrónico

Deliberações

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

- Deliberação n.º 61/2004 - Princípios do tratamento de dados por videovigilância [Em linha], Lisboa, 19 de abril de 2004. [Consultado 4 julho 2014]. Disponível em WWW: <URL: http://www.cnpd.pt/bin/orientacoes/DEL61-2004-VIDEOVIGILANCIA.pdf>.

- Deliberação n.º 227/2007 - Tratamento de dados efetuados no âmbito de estudos de investigação científica na área da saúde [Em linha], Lisboa, 28 de maio de 2007. [Consultado 4 julho 2014]. Disponível em WWW: <URL:http://www.cnpd.pt/bin/orientacoes/DEL227-2007-ESTUDOS-CLINICOS.pdf>.

- Deliberação n.º 333/2007 - Proteção de dados pessoais nos ensaios clínicos com medicamentos de uso humano [Em linha], Lisboa, 16 de julho de 2007. [Consultado 4 julho 2014]. Disponível em WWW: <URL: http://www.cnpd.pt/bin/orientacoes/DEL333-2007-ENSAIOS-CLINICOS.pdf>.

- Deliberação n.º 629/2010 - Tratamento de dados de gravação de chamadas [Em linha], Lisboa, 13 de setembro de 2010. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://www.cnpd.pt/bin/orientacoes/DEL629_2010.pdf>.

- Deliberação n.º 840/2010 - Tratamentos de dados no âmbito da gestão da informação dos serviços de segurança e saúde no trabalho [Em linha], Lisboa, 11 de outubro de 2010. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://www.cnpd.pt/bin/orientacoes/DEL_840_2010_MED_trabalho_actualizada.pdf>.

- Deliberação n.º 890/2010 - Tratamentos de dados com a finalidade de medicina preventiva e curativa no âmbito do controlo de substâncias psicoativas efetuados a trabalhadores [Em linha], Lisboa, 15 de novembro de 2010. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://www.cnpd.pt/bin/orientacoes/20_890_2010.pdf>.

- Deliberação n.º 1638/2013 - Controlo da utilização para fins privados das TIC no contexto laboral [Em linha], Lisboa, 16 de julho de 2013. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf>.

Pareceres

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS - Parecer n.º 18/2000 [Em linha], Lisboa, 2 de maio de 2000. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://www.cnpd.pt/bin/decisoes/2000/htm/par/par018-00.htm>.

GRUPO DE TRABALHO DO ARTIGO 29º

- Parecer n.º 4/2004 - Tratamento de dados pessoais por meio de videovigilância [Em linha], Bruxelas, 11 de fevereiro de 2004. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp89_en.pdf>.

- Parecer n.º 4/2007 - Conceito de dados pessoais [Em linha], Bruxelas, 20 de junho de 2007. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_pt.pdf>.

- Parecer n.º 3/2013 - Limitação da finalidade no tratamento de dados pessoais [Em linha], Bruxelas, 2 de abril de 2013. [Consultado a 4 julho 2014]. Disponível em WWW: <URL:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

Página propositadamente deixada em branco

Jurisprudência

- Acórdão do Supremo Tribunal de Justiça, 3ª Secção, de 28 de setembro de 2011 (Processo n.º 22/09.6YGLSB.S2), relatado por Santos Cabral (disponível em http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/25cd7aa80cc3adb0802579260032dd4a?OpenDocument&Highlight=0,22%2F09.6YGLSB.S2).

- Acórdão do Tribunal Constitucional, decidido em Plenário, de 12 de junho de 2002 (Processo n.º 696/96), relatado pelo Conselheiro Guilherme da Fonseca.

- Acórdão do Tribunal da Concorrência, Regulação e Supervisão, 1º Juízo, de 21 de outubro de 2013 (Processo n.º 140/13.6YUSTR), relatado por Marta Campos.

- Acórdão do Tribunal da Relação de Évora, Secção Criminal, de 24 de abril de 2012 (Processo n.º 932/10.8PAOLH.E1), relatado por Maria Filomena Soares (disponível em http://www.dgsi.pt/jtre.nsf/134973db04f39bf2802579bf005f080b/c7875c514b7fa32a802579ff003e21b7?OpenDocument&Highlight=0,imagens,como,meio,de,prova).

- Acórdão do Tribunal da Relação de Lisboa, 9ª Secção, de 30 de outubro de 2008 (Processo n.º 8324/2008-9), relatado por Margarida Veloso (disponível em http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/c222f7dd896e84da802575010043b3dc?OpenDocument&Highlight=0,videovigil%C3%A2ncia,como,meio,de,prova).

- Acórdão do Tribunal da Relação do Porto, 1ª Secção, de 26 de março de 2008 (Processo n.º 0715930), relatado por Joaquim Gomes (disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/24cd01e84ff51ff88025741e0034cc7e?OpenDocument&Highlight=0,imagens,como,meio,de,prova).

- Acórdão do Tribunal da Relação do Porto, 4ª Secção, de 23 de outubro de 2013 (Processo n.º 585/11.6TABGC.P1), relatado por Maria do Carmo Silva Dias (disponível em http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/301ec6a6cdd8ceab80257c1a005a61e4?OpenDocument&Highlight=0,imagens,como,meio,de,prova).

Índice de referências jurisprudenciais

Acórdão do Tribunal Constitucional, de 12 de junho de 2002 (Processo n.º 646/96)……..58

Acórdão do Tribunal da Concorrência, Regulação e Supervisão, de 21 de outubro de 2013 (Processo n.º 140/13.6YUSTR)…….60

Acórdão do Tribunal da Relação do Porto, de 26 de março de 2008 (Processo n.º 0715930)……95

Acórdão do Tribunal da Relação do Porto, de 23 de outubro de 2013 (Processo n.º 585/11.6TABGC.P1)…….95

Acórdão do Tribunal da Relação de Évora, de 24 de abril de 2012 (Processo n.º 932/10.8PAOLH.E1)…….....96

Acórdão do Tribunal da Relação de Lisboa, de 30 de outubro de 2008 (Processo n.º 8324/2008-9)…….....96

Acórdão do Supremo Tribunal de Justiça, de 28 de setembro de 2011 (Processo n.º 22/09.6YGLSB.S2)…….....97

Página propositadamente deixada em branco

Índice geral

1. Introdução…….13

2. Caraterização da Comissão Nacional de Protecção de Dados

2.1. A CNPD no âmbito nacional……15

2.2. A CNPD no âmbito internacional

2.2.1. Instância Comum de Controlo da Europol…….17

2.2.2. Autoridade de Controlo Comum Schengen……17

2.2.3. Autoridade Supervisora Comum do Sistema de Informação Aduaneira……....18

2.2.4. Grupo de Trabalho das Telecomunicações…….19

2.2.5. Grupo de Trabalho de Proteção de Dados……..19

3. Estágio

3.1. Duração e faseamento……...21

3.2. Expetativas anteriores à realização do estágio……....22

3.3. Relevância atribuída ao estágio……..22

4. **Descrição das atividades desenvolvidas**……..…....25

4.1. Conceito de dados pessoais segundo a opinião 4/2007, de 20 de junho, do Grupo de Trabalho do Artigo 29º……....26

4.2. Princípio da limitação da finalidade segundo a opinião 3/2013, de 2 de abril, do Grupo de Trabalho do Artigo 29º……...32

4.3. Privacidade no local de trabalho

4.3.1. Tratamentos de dados no âmbito da gestão da informação dos serviços de segurança e saúde no trabalho……...34

4.3.2. Tratamentos de dados com a finalidade de medicina preventiva e curativa no âmbito dos controlos de substâncias psicoativas efetuados a trabalhadores……36
4.3.3. Tratamentos de dados decorrentes da utilização para fins privados das tecnologias de informação e comunicação no contexto laboral…….38
4.3.3.1. Os tratamentos de dados em particular
A. Princípios relativos ao controlo de dados de comunicações telefónicas e de dados de tráfego……..40
B. Princípios relativos ao controlo do correio eletrónico…….40
C. Princípios relativos à internet……....41
4.4. Tratamento de dados de saúde
4.4.1. Tratamentos de dados efetuados no âmbito de estudos de investigação científica na área da saúde……...42
4.4.1.1. Particularidades do consentimento…….....45
4.4.2. Tratamentos de dados no âmbito de ensaios clínicos com medicamentos de uso humano……46
4.4.3. Tratamentos de dados com a finalidade de prescrição eletrónica de medicamentos e gestão do processo clínico……49
4.4.4. Tratamentos de dados com a finalidade de gestão de utentes…..50
4.5. Tratamentos de dados na gravação de chamadas……...50
4.6. Tratamentos de dados com a finalidade de cessão de créditos……...54
4.7. Videovigilância
4.7.1. Tratamentos de dados por meio de videovigilância segundo a opinião 4/2004, de 11 de fevereiro, do Grupo de Trabalho do Artigo 29º……...56
4.7.2. Princípios sobre o tratamento de dados por videovigilância segundo a Deliberação n.º 61/2004, de 19 de abril, da CNPD……58

4.7.3. Processo de contraordenação por realização de tratamento de dados decorrente da instalação e utilização ilegítima de equipamentos de videovigilância……60
4.8. Gabinete de Atendimento ao Público: questões suscitadas……64

5. Análise crítica das atividades desenvolvidas

5.1. Legislação de proteção de dados pessoais: evolução e relevância na proteção da privacidade……65
5.1.1. Na Europa……..66
5.1.2. Nos Estados Unidos……...69
5.1.3. Em Portugal…….....70
5.2. Medidas de segurança nos tratamentos de dados……...74
5.3. Responsável pelo tratamento de dados……..76
5.4. Direitos dos titulares dos dados
5.4.1. Direito ao esquecimento…….....77
5.4.2. Direito à curiosidade……...77
5.4.3. Direito de informação…….....77
5.4.4. Direito de acesso…….....78
5.4.5. Direito de retificação e atualização……..78
5.4.6. Direito de apagamento ou bloqueio dos dados……...79
5.4.7. Direito de não ficar sujeito a uma decisão individual automatizada……...79
5.4.8. Direito de oposição……79
5.5. Confidencialidade no tratamento de dados……....80
5.6. Condições de legitimidade para o tratamento de dados
5.6.1. Tratamento de dados sensíveis……....81
5.6.2. Tratamento de dados relativos a suspeitas de atividades ilícitas, infrações penais e contraordenacionais……....82
5.6.3. Tratamento dos dados que não se incluem nas categorias acima descritas……..82
5.7. Princípios da proteção de dados pessoais
5.7.1. Princípio da transparência……...84

5.7.2. Princípio da finalidade ou da especificação da finalidade…….84
5.7.3. Princípios relativos à qualidade dos dados
A. Princípio da licitude e da lealdade……....85
B. Princípio da adequação, pertinência e proporcionalidade……85
C. Princípio da exatidão e atualização dos dados……..85
5.8. Videovigilância – análise dos casos suscitados no Gabinete de Atendimento ao Público……...86
5.8.1. Câmaras em ginásios que funcionam em horários noturnos……87
5.8.2. Controlo de desempenho profissional de trabalhadores por meio de câmaras de videovigilância……..89
5.8.3. Utilização como meio de prova de imagens captadas por sistemas de videovigilância não legalizados……....92
5.8.4. Controlo oculto por meio de videovigilância……...98
5.9. Consequências do desrespeito pelas normas de proteção de dados…….…...100

6. Conclusão……...103

Bibliografia……..……...107

Jurisprudência…….……...…113

Índice de referências jurisprudenciais……..……....115

Índice geral..……...117